

CONTENTS

HIGH TECHNOLOGY LAW JOURNAL

VOLUME 10 NUMBER 2 1995

ARTICLES

The Commercial Law of Internet Security

Michael Rustad and Lori E. Eisenschmidt 213

Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents

Timothy J. Douros 321

COMMENTS

Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics

Joseph M. Reisman 355

A Behavior-Based Model for Determining Software Copyright Infringement

Dennis M. Carleton 405

BOOK REVIEW

DNA in the Courtroom: A Trial Watcher's Guide by Howard C. Coleman and Eric D. Swenson

Reviewed by Jasmine Samrad 433

INDEXES

Author Index 447

Issue Index 460

Subject Index 466

Title Index 475

ARTICLE

THE COMMERCIAL LAW OF INTERNET SECURITY

MICHAEL RUSTAD [†] AND LORI E. EISENSCHMIDT ^{††}

TABLE OF CONTENTS

I.	INTRODUCTION	214
II.	STATE-OF-THE-ART NETWORK SECURITY.....	218
	A. The Technical Elements of Network Security	220
	B. The Internet/Network Security Industry.....	239

© 1995 Michael Rustad & Lori E. Eisenschmidt.

[†] Professor of Law, Suffolk University Law School; LL.M., 1986, Harvard University; J.D., 1984, Suffolk University Law School; Ph.D., 1981, Boston College. Prof. Rustad teaches courses in commercial law, torts and high technology law. He is a member of the American Law Institute and a Task Leader of the ABA Business Law Section's Subcommittee on Software Contracting. He is Co-Chair of the Task Force on General Provisions of the Proposed U.C.C. Article 2B on the licensing of intangibles.

^{††} J.D. Candidate, 1996, Suffolk University Law School; B.A., 1985, University of South Florida. Ms. Eisenschmidt co-authored working papers on tort law and security with Professor Rustad for the ABA Science and Technology Section's Law and Ethics on the 'Nets project ("Project LEON") in the Spring of 1995.

The authors gratefully acknowledge the exhaustive technical consultation and review provided by Harold H. Leach, Jr., J.D., LL.M. Mr. Leach is a principal in the Boston-based computer consulting firm Legal Computer Solutions, Inc. His firm specializes in automating law firms and legal departments. Mr. Leach was formerly a partner at the Boston law firm of Choate, Hall & Stewart. The authors would like to thank Professor Jeffrey Atik of Suffolk University Law School and Ellen Kirsh, Vice President and General Counsel of America Online, Inc., for providing materials and valuable suggestions. We would also like to thank Barry Nelson, a former BBN systems engineer and current third-year student at Suffolk University Law School, for his critical reading and editorial assistance. Fourth-year evening students Charles Rosenthal and Elaine Martel were instrumental in the design and execution of the Computer Law Association Survey. The valuable research assistance of Kizuki Kuzuhari, F.A. Lichauco and Chris Palmisano should also be acknowledged. We would also like to thank the reference librarians of Suffolk University Law School. Finally, our thanks and appreciation are extended to Sylvia Michaud for unflagging administrative assistance. The opinions expressed in this paper should not be attributed to our colleagues or institutions.

III. THE QUESTION OF LEGAL STANDARDS FOR INTERNET SECURITY	243
A. Regulation Under Tort Law	244
B. Regulation Under Current Contract Law	262
IV. REGULATION OF INTERNET SECURITY PRODUCTS UNDER PROPOSED U.C.C. ARTICLE 2B.....	274
A. Anatomy of Proposed U.C.C. Article 2B	278
B. The Case for Adopting the Proposed Article 2B for Internet Security Software.....	293
V. CONCLUSION	300
VI. APPENDIX A: EXAMPLE OF SALES AND LICENSE AGREEMENT OF A NETWORK SECURITY PRODUCT	302
VII. APPENDIX B: COMPUTER LAW ASSOCIATION SURVEY AND RESULTS.....	313

I would not want to depend on the Internet for the livelihood of my business The reality is that Internet security is basically an oxymoron.¹

Security on the Internet is a solved issue. By year's end, off-the-shelf products will be available to ensure secure Internet transactions.²

I. INTRODUCTION

Since the Clinton administration endorsed the establishment of a National Information Infrastructure (NII),³ the rise in Internet use has been meteoric. As of July 1995, the Internet links an estimated thirty million users, and the number of users continues to grow an astonishing 20% per month.⁴ In the past decade, the Internet has grown from

1. Laurent Belsie, *Computer Theft Cases Show Holes in Internet*, CHRISTIAN SCIENCE MONITOR, Mar. 1, 1995, at 3 (quoting Daniel White, Partner, Ernst & Young).

2. Peggy Liu, Product Manager, NetManage, Inc., Presentation at 1995 Spring Workshop: Internet and the Entrepreneur, MIT Enterprise Forum of Cambridge, Inc. (Apr. 22, 1995).

3. John Byczkowski, *U.S. Grappling with Access to Information*, CINCINNATI ENQUIRER, Mar. 7, 1995, at B06; Calvin Reid, *Publishers Support Clinton Report on Copyright, Cyberspace. 'Intellectual Property and the National Information Infrastructure' Report Recommends Limited Amendments to the Copyright Act to Properly Protect New Technologies*, 242 PUBLISHERS WKLY. 11 (Sept. 11, 1995).

4. April Streeter, *Don't Get Burned By the Internet*, LAN TIMES, Feb. 13, 1995, at 58 (quoting 20% growth figure provided by the Carnegie Mellon University Computer Emergency Response Team); Arthur Middleton Hughes, *Internet DB Marketing with*

1,000 end-user computers to greater than two million.⁵ The development of the World Wide Web (WWW or Web), an increasingly interactive medium supporting high-resolution color graphics and multimedia presentations, has fueled this growth. Of the already thirty million Internet users, a minimum of fifteen million have access to the World Wide Web.⁶ The Web is projected to have just under twenty-two million users by the turn of the century.⁷

In addition to individuals, large and small corporations, law firms and legal departments, and specialty boutiques and consultant service providers are discovering the power of the Internet. Advances in technology and user-friendly access have made it more desirable and economically feasible to connect parent and subsidiary corporations through the Internet instead of through more expensive private networks. Strategic business alliances are using the Internet for global networking and data transfers. Even advertising is finding a niche—the cost of advertising on the Web is “minuscule” relative to that of advertising in a newspaper, and advertisers have access to millions of Internet users.⁸

Amidst the surging excitement and interest, however, runs a deep thread of ambivalence toward connecting to the Internet. The Internet’s evil twin is the home of “Bad Guys”—hackers,⁹ crackers, snackers, stalkers, phone phreaks and other creepy Web crawlers.¹⁰ Businesses fear that the Infobahn could suddenly veer into the highway to Hell.¹¹ Insincere and downright devious transactions by malefactors may cause a firm to unwittingly disclose its prime

CD-ROMs, *DM NEWS*, Aug. 21, 1995, at 22 (stating that the network consists of “almost five million” server computers).

5. Richard Raysman & Peter Brown, *On-Line Legal Issues*, N.Y. L.J., Feb. 15, 1995, at 30.

6. Hughes, *supra* note 4, at 1.

7. Belsie, *supra* note 1, at 3 (quoting Forrester Research, Inc.).

8. Arnold Kling, *Mortgages over the Internet*, 55 *MORTGAGE BANKING* 18 (Nov. 1994); *CompuServe*, *NMAA Sign Multimillion-Dollar Internet Access Agreement; NMAA Members Offered Free Internet Test-Drive*, *PR NEWSWIRE*, Aug. 21, 1995.

9. This article uses “hacker” to encompass any malevolent intruders. Historically, however, it should be understood that the term “hacker,” “coined at MIT in the 1960s, simply connoted a computer virtuoso.” Wade Roush, *Hackers: Taking a Byte Out of Computer Crime*, *TECH. REV.*, Apr. 1995, at 32. Internet cultural anthropologists distinguish between crackers, snackers and hackers. Technically, “crackers” thrive on the challenges of breaking in, “snackers” try to see what is interesting, and “hackers” intrude for the intellectual curiosity of understanding how things work.

10. Maggie Cannon, *Life in the Big City: Internet Concerns*, *MACUSER*, May 1995, at 17 (describing creepy characters residing on the Infobahn).

11. Internet deviants have captured the imagination of mass culture. For example, Fox Television Network has a new series featuring a New York City undercover cop who tracks an Internet stalker. *ENTERTAINMENT WKLY.*, Sept. 15, 1995, at 73.

information commodities. Bad Guys could enter a firm's computer through the Internet connection and steal or compromise a firm's informational crown jewels.¹² Valuable information includes not only a company's marketable information products such as software, but also proprietary information such as customer lists, product designs, marketing plans and other trade secrets. Since this information is increasingly entrusted to, circulated on and stored in computer systems,¹³ the critical question is: "Just how secure is the Internet?"

Examples of hacker malfeasance and Internet insecurity are legion.¹⁴ A recent electronic bulletin board service survey reported that 69% of the respondents' firms perceived significant security threats.¹⁵ Half of those respondents reported theft of property of \$10,000 or more.¹⁶ Around 18% of the respondents reported that their firm was victimized by fraudulent computer activity by a trusted party or insider.¹⁷ Approximately 10% reported fraudulent losses to outsiders.¹⁸ About 93% of the responding firms had implemented a network security project.¹⁹

One Internet user purportedly set up an anonymous file-transfer protocol²⁰ (FTP) site called "INFES-Station BBS" that was allegedly intended to distribute virus code.²¹ Another hacker reportedly stole a number of sophisticated computer programs which may be used to unscramble cellular-telephone codes and to facilitate infiltration of

12. See David Bernstein, *Insulate Against Internet Intruders*, DATAMATION, Oct. 1, 1994, at 49.

13. Senator Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH. 1, 21 (1992) ("The maintenance of the security and integrity of computer systems has become increasingly critical to interstate and foreign commerce, communications, education, science, technology, and national security. As we move even further into the hi-tech age, we depend on computers to process essential information and to store it in a manner in which it will not be altered.").

14. One security expert finds scavenging, leakage, piggybacking, wire tapping, data diddling, viruses and salami-type thefts to be quite common. See generally RICHARD H. BAKER, NETWORK SECURITY: HOW TO PLAN FOR IT & HOW TO ACHIEVE IT 183 (1995).

15. *Id.* at 183-84 (reporting survey of COMSEC BBS).

16. *Id.* at 184.

17. *Id.*

18. *Id.*

19. *Id.*

20. Protocols are electronic communications "rules" which allow for the orderly, reliable transfer of data. A file-transfer protocol permits transfers of files between computers with unique software and hardware configurations. Other examples of protocols are the International Standards Organization (ISO) and the standard ASCII character set.

21. Gary H. Anthes, *Internet Triggers Virus Debate, Security Measures; Providers Dispute Accountability for Virus Distribution*, COMPUTERWORLD, Feb. 27, 1995, at 66.

other computers.²² Pentagon officials recently disclosed that, in a 1994 internal audit of their network security, an in-house team employing hacker techniques successfully penetrated 88% of the 8,900 government computers they attacked, with only 4% of the break-ins being detected.²³

Increased business activity on the Internet is likely attracting hacker activity.²⁴ Some malefactors hack business sites for the same reason Willie Sutton robbed banks: "That's where the money is."²⁵ Researchers at Carnegie Mellon University report that the increase in attempted intrusions to Internet hosts parallels the monthly rise in Internet connections.²⁶ By one estimate, the number of Internet break-ins has increased by more than 70% in each of the last two years.²⁷ Because of such security concerns, a December 1994 survey reported that many firms were deciding against connecting to the Internet.²⁸

The security risks of connecting to the Internet raise a number of legal questions not yet resolved by case law or commentary.²⁹ A large number of network security products has recently appeared on the market which claim to have solutions to the problem of the "Bad Internet."³⁰ One new security product was described as "close to the level of 'bullet-proof'."³¹ Some firms have even represented their

22. Michael Myer et al., *Stop! Cyberthief! Technology: Don't Be Alarmed, But the Law Can't Cope With Computer Crime*, NEWSWEEK, Feb. 6, 1995, at 36. These programs belonged to Tsutomu Shimomura and the San Diego Supercomputer Center. *Id.*

23. Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C03.

24. Streeter, *supra* note 4, at 58 (quoting Bill Pozerycki, Internet security service manager, Digital Equipment Corp., Maynard, Massachusetts).

25. This apocryphal statement should not be misconstrued as implying that the sole motivation behind all hacking is money. As explained in *supra* note 9, Internet cultural anthropologists differentiate among varying types of hackers according to their motivations.

26. Streeter, *supra* note 4, at 58.

27. Belsie, *supra* note 1, at 3.

28. *Internet World Investigates High Tech Security on the Internet*, BUSINESS WIRE, Dec. 19, 1994.

29. See generally I. Trotter Hardy, *The Proper Legal Regime for 'Cyberspace'*, 55 U. PITT. L. REV. 993, 994 (1994). See also Lawrence Lessig, *Symposium: Emerging Media Technology and the First Amendment: The Path of Cyberlaw*, 104 YALE L.J. 1743 (1995).

30. See Anne Knowles, *UUNet Suite Tightens Security: System Offers Firewall, Encryption for Virtual Private Networks*, PC WEEK, May 29, 1995, at 14; Erica Roberts, *Network Systems to Secure Hubs, Routers*, COMM. WEEK, Feb. 20, 1995, at 1 [hereinafter Roberts, *Network Systems*]; Erica Roberts, *Easing LAN Access to the Internet*, COMM. WEEK, Feb. 13, 1995, at 27; Streeter, *supra* note 4, at 58.

31. *Network Systems Offers Public, Private Network Data Security*, NETWORK MANAGEMENT SYSTEMS & STRATEGIES, Nov. 15, 1994, at 1043.

product(s) to be "hacker-proof."³² Because of the lag between the legal infrastructure and the new network security technologies, it is completely uncertain whether representations such as these would be deemed enforceable by a court of law.

This article examines a vital problem of the information technologies—the unresolved legal dilemmas arising out of the development of network security technologies. To understand the legal dilemmas raised by the new network security technologies, we first need an overview of how the technologies work. Part II of this article describes the components which comprise Internet security and reviews the state-of-the-art security devices and methods available to combat Internet abuse. It then reviews the spectrum of security products and the emerging network security industry.

Part III identifies the plight of courts, policy makers and vendors and vendees by setting forth key legal issues that arise out of these new technologies. Failure to resolve these legal dilemmas would result in the delay of the development of network security products serving the NII and the NII itself. Part III also provides a discussion of traditional tort and contract law, plus Article 2 of the Uniform Commercial Code (U.C.C.), as they might be applied to resolve these issues.

Part IV advocates the forthcoming licensing article (Article 2B) of the U.C.C. as a legal framework ideally suited for the resolution of the novel and complex issues posed by the marketing of Internet information security products. We contend that the emerging software licensing law is a flexible body of law adaptable for resolving numerous information technology issues. We assess the rules of the proposed Article 2B for providing a coherent legal framework for security network products. Since the proposed Article 2B alone cannot manage all liability concerns, we recognize a residual role for tort law for cases of market failure and for vindicating the rights of third parties injured by security breaches. Tort liability will also come into play if there is an independent tort arising out of a breach of contract. However, too much tort law may be detrimental to the continued development of the NII.

II. STATE-OF-THE-ART NETWORK SECURITY

"Network security" is much like home security. Precautions and safeguards are scaled to the level of risk. In a crime-free world, the

32. Roberts, *Network Systems*, *supra* note 30, at 1 (statement of Tom Gilbert, marketing director at Network Systems Corp.) ("We have comprehensive solutions . . . to provide hacker-proof security across any network.").

beginning and end of home security might be painting and weatherstripping the house—insulating against the elements and taking precautions to guard against fire and natural disasters. In such a neighborhood, intruder invasion is not a concern. The world, of course, is not a crime-free place, and neither is “Cyberspace.”³³ Just as products, devices and methods (such as locks, steel doors, security monitors and guards) have been developed and marketed to protect homes against unwarranted intrusion, an entire industry is arising to develop products and protocols designed to deter electronic invasion of computer systems.

Computer (or network) security differs from home security in two important respects. First, home security is primarily designed to prevent the theft of tangible items of property. In contrast, the network security industry must address the electronic, intangible nature of the computer data it seeks to protect. Even though the physical disks or diskettes used in connection with computers are tangible, the electronic data on them is a formless collection of magnetically-fixed electronic impulses. The network security industry’s objective is to protect this treasure trove of magnetic data from unwanted intrusion and theft. Were it not so, security for computers could be limited to physical harm and theft prevention, much like security for typewriters.

The second but related difference concerns the interconnectivity of computers. Unlike a home burglar, an intruder does not need to have *physical* access to a computer in order to effectuate an unauthorized entry; *electronic* access can suffice. Computers can be connected by wires, via modem and telephone lines, or even via the Internet. Once connected, computers and their precious data are potentially accessible to remote intruders, if appropriate security measures are not taken. This part lays out the basic principles underlying these inter-networking technologies, explores the various components of network security, and finally, discusses the role of the network security industry.

33. William Gibson coined the term “Cyberspace” in his 1984 science fiction book *Neuromancer* to describe the “virtual world created by a computer system.” Michael D. Scott, *Advertising in Cyberspace: Business and Legal Considerations*, COMPUTER LAWYER, Sept. 1995, at 1 n.1 (discussing WILLIAM GIBSON, *NEUROMANCER 2* (1984)). “Cyber” is derived from the Greek word “*kybernan*,” which means “to steer or control.” *Id.*

A. The Technical Elements of Network Security

1. CLIENT AND SERVER COMPUTERS

In order to develop a coherent legal regime for network security products, it is necessary to understand the basic principles underlying networking technologies. The degree of risk of Internet abuse depends on the method of Internet connectivity, the type of computer hardware used, the number and type of security devices in use, and the nature of the user (e.g., educational institution, government entity, business or home). In general, the risk factor is less for computers which access the Internet via an Internet service provider (ISP) than for computers which have direct access to the Internet. In addition, companies and governmental offices are most likely to be targeted by hackers, followed by educational institutions and homes.³⁴

The current trend is for businesses to link intracompany computers together by wire or cable to form a Local Area Network (LAN).³⁵ Software designed for a LAN permits linked computers to share programs and data files, and to exchange electronic mail (e-mail). It also permits shared printers, plotters, imaging devices, hard disks and other transfer and device concepts. The LAN comprises a mini-"data highway" with one of the computers acting as the resource manager or "server."³⁶

Any stand-alone IBM compatible personal computer (PC) or Macintosh computer (Mac) with a modem is an example of a simple "client" computer. The client computer typically connects to the Internet by establishing a telephone connection to an ISP computer. The ISP computer functions as a "server" computer, providing news and mail services, as well as routing data between the client computer and the rest of the Internet.³⁷ Server computers are connected by

34. Because government and business computer networks are more sophisticated and more closely guarded than home or school computer networks, hackers find the challenge of penetrating them more appealing. In addition, hackers seeking financial gain are more likely to reap substantial rewards from government or business computers than from home or school computers.

35. The rise of low-cost microcomputers in the 1980s facilitated the growth of LANs. IBM lost ground because of its failure to predict the decline of the mainframe computer and the rise of the LAN. Today, the desktop work station is the computer industry's *de facto* standard for software development.

36. The term "server" refers to any device which offers a service to network users.

37. ISPs with "dial-up" services are available in most cities. For example, in the Boston Metropolitan area, Internet connectivity services are available from North Shore Access of Lynn; Novalink of Westborough; and The Internet Access Co. of Bedford, to name a few. America Online, CompuServe and other commercial services have recently begun offering Internet access for use by their individual and business customers.

high-speed telephone lines to the network of computers which comprise the backbone of the Internet. The ISP's server computer is "on" the Internet twenty-four hours a day. Any computer "on" the Internet may be potentially "hacked into" from elsewhere on the Internet by the Bad Guys.

The popular wisdom is that a pure "client" computer or "client" computer network is a super-hero, easily able to keep out the Internet Bad Guys. It is shielded by an intermediary—the ISP server computer. Even if the ISP server is compromised, the client computer is still safe, because it lacks the communications protocols necessary to enable the hacker to establish a connection with it. Yet, if the client computer connects to the ISP computer via a Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) connection, it is likewise "on" the Internet and may be vulnerable to attack. This vulnerability, however, does not arise unless the client computer itself runs programs which allow it to act as a server.³⁸

The greatest threat to the security of client computers is not the Internet hacker, but rather the enemy within, the in-house hacker. Insiders who have high level computer-access privileges may abuse them. Insiders who have otherwise nominal access privileges can invade the computer system by "shoulder surfing," intercepting passwords of individuals with higher-level clearance. In this context, PC- and Mac-based LANs are more vulnerable to internal security breach than are mainframe computers: mainframe computer systems have traditionally had a department of Management Information Systems (MIS) dedicated to backups and security; no such tradition exists in the LAN environment.³⁹

2. ROUTERS/GATEWAYS

Many large companies and educational institutions equip their computers or LANs with "routers."⁴⁰ Routers allow them to access the Internet "directly," perhaps in combination with a gateway, rather than dialing-up and going through an ISP. Routers/gateways filter messages which are destined for recipients outside the local network.

38. Such a program is referred to in the industry as a "daemon-program."

39. *Network Help Desk*, NETWORK WORLD, Nov. 21, 1994, at 2.

40. A router is a device which employs special communications protocols. The protocols enable, at a minimum, the passing of information from the Internet to LAN destinations, and vice versa. A gateway may also be used if the LAN does not recognize Internet protocols such as System Network Architecture. The gateway performs the function of converting the disparate networks' protocols to the one compatible to its system. Additional protocols can be added to enable error detection and connection bookkeeping functions.

and receive messages from remote networks to be delivered locally on the LAN. Just as a group of computers in an office can be linked together to share files and e-mail through a LAN, LANs can themselves be networked on a world-wide scale. A multi-national corporation located in the Netherlands can thus be linked to its subsidiaries in England and South Africa via the Internet. Via the router/gateway, the companies' computers can send and receive electronic data and requests "directly" from the Internet.

It is important to note that companies and institutions connected to the Internet via a router/gateway are "on" the Internet, much like ISPs are directly on the Internet. They are thus at risk from Internet hackers. Because of this, if proper security precautions are not taken by the computer systems administrator (SysAdmin), the router/gateway may be the most vulnerable point in a company's network.

3. OPERATING SYSTEM

Security on the Internet is inseparable from the security of the computers that access and/or serve the Internet. At the server level, security can be breached on several fronts. The first vulnerability lies with the ISP hardware's operating system (O/S). The majority of the computers connecting the Internet use Unix-based or compatible standardized operating systems. Unix-based O/Ss were not originally designed with security in mind; they contain scores of well-known, documented security "loopholes." In addition, hackers occasionally discover new methods for circumventing supposedly secure aspects of the O/S.⁴¹ They may exploit such O/S weaknesses to gain some measure of unauthorized access and control.

For example, if a hacker penetrates an Internet service provider's O/S, he will be able to access at least some data stored on the ISP's computer. Depending on the severity of the loophole he has uncovered, he may be able to: access and copy a list of the server's accounts (i.e., the computers/companies which utilize that ISP to access the Internet); browse e-mail stored on the computer for some or all of the accounts; or disclose or damage ISP data files. In cases of severe breach, he can actually disrupt or halt the operation of the server's programs, and may be able to extend his destructiveness to other computers by introducing a malicious routine, such as a computer

41. The U.S. Government has funded the Computer Emergency Response Team (CERT) to track vulnerabilities and to warn SysAdmins to fix them. CERT issues security advisories which may be read on-line in the "comp.security.announce" newsgroup, or which may be sent directly to an individual or organization's e-mail account by subscribing to CERT's free mailing list.

"virus" or "worm."⁴² Worms and viruses are programmed to propagate their havoc automatically, ad infinitum.⁴³

Various means exist for ferreting out and plugging security holes at the O/S level.⁴⁴ SysAdmins can self-administer programming tools to search for vulnerabilities in their systems. Alternatively, a company may choose to hire a computer firm or consultant specializing in security to run the programs and/or perform a complete security analysis. Internet Security Systems, Inc. markets "Internet Scanner," purportedly the "most comprehensive 'attack simulator' available."⁴⁵ Its software "systematically probes an organization's network for security holes, providing a vulnerability report on each device on the network with recommendations for corrective action."⁴⁶ Internet Scanner scans for over 100 security vulnerabilities.⁴⁷

Other examples of diagnostics products include the controversial "Security Administrator Tool for Analyzing Networks" (SATAN) program, "COPS," "OmniGuard/Enterprise Access Control for Unix," and "NetProbe." SATAN's dual nature makes it controversial: because it functions by probing its target across the network from another host, it can be used to crack systems as well as to defend them.⁴⁸ Using SATAN, a hacker can systematically exploit any known system weakness which has not been remedied.⁴⁹ The other scanners run directly on the target host and operate as self-diagnostics.⁵⁰ SATAN and COPS can be downloaded from various servers on the Internet and used for free; the others are available

42. "Worm" and "virus" are defined as follows:

[A] "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.

United States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir.), cert denied, 502 U.S. 817 (1991).

43. John DeHaven, *State of the Art: Seeking Security Stealth Virus Attacks*, BYTE, May 1, 1993, at 137.

44. See generally ANDRE BACARD, *COMPUTER PRIVACY HANDBOOK* (1995); *IMPLEMENTING INTERNET SECURITY*. (Frederic J. Cooper et al., eds., 1995).

45. Thomas Noonan *Joins Internet Security Systems as President*, BUSINESS WIRE, Aug. 30, 1995.

46. *Id.*

47. *Id.*

48. Jason Levitt, *Techview: Dealing With the Devil*, INFORMATION WEEK, Apr. 17, 1995, at 42.

49. See Winn Schwartau, *The Key to Defeating SATAN is Understanding How It Can Bedevil You*, NETWORK WORLD, May 1, 1995, at 32.

50. Rkutrell Yasin, *Vendors Fire Up Wares to Vie with SATAN*, COMMUNICATIONS WEEK, Apr. 10, 1995, at 4.

commercially. Properly utilized, both types of products enable SysAdmins to find and plug O/S security holes before hackers can exploit them.

Since Unix-based O/Ss have numerous inherent security flaws, informal norms in the industry have filled the gaps. Some of the widely-shared industry practices include: monitoring for hacker programs,⁵¹ worms and viruses;⁵² blocking repetitive failed access attempts; maintaining adequate log-in and audit trail records,⁵³ and monitoring for other indicia of trouble. Now that extensive means are available to overcome the original security loopholes, operating system security is a "reasonable" proposition.⁵⁴

Other O/Ss, such as Digital Equipment Corporation's Open VMS/VAX 6.0 and Security Enhanced VAX/VMS, have been evaluated by the Department of Defense's National Computer Security Center (NCSC) and rated as meeting or exceeding security

51. One virulent hacker program permits the storage of a copy of a user's log-in for later retrieval and use by the hacker.

52. McAfee, which commands a 67% world-wide market share in virus detection products, offers "VirusScan" for non-Unix-based client and server computers. Its technology allows accurate detection of over 5,100 known and new viruses, including "boot viruses, file viruses, multi-partite viruses, stealth viruses, encrypted viruses, and polymorphic viruses." The company maintains a 24-hour Virus Emergency Response Center. *McAfee Releases VirusScan for Windows 95 and Announces Windows NT Support*, BUSINESS WIRE, Aug. 18, 1995. See also "<http://www.mcafee.com/a-v/pub/vscan.html>."

The leading European anti-virus software is "Dr. Solomon's Anti-Virus Toolkit," made by S&S Software International, Inc. It detects and "kills" more than 6,700 computer viruses. S&S Software International maintains a research team which detects 150 to 200 new viruses a month. The team provides 24- to 48-hour virus identification and also repair, if possible. The team has devised a downloadable program for Toolkit users for detecting the prolific new macro-based virus known variously as "WinWord.Concept," "WW6Macro," and "Prank Macro." They have also prepared a white paper with instructions on how to remove the virus. While specializing in security and networking products for IBM-compatible systems, S&S International is expected to release Macintosh, SCO UNIX, Windows 95, Windows NT Server and Windows NT Workstation versions of Toolkit in the fall of 1995. *New Computer Virus Infects Winword 6 Users; S&S Releases Fix for World's First Macro Virus*, PR NEWSWIRE, Aug. 30, 1995. See also "<http://www.drsolomon.com>."

53. Hackers' failed access attempts are often recorded on log on and audit trail records. The auditing function of security programs enables SysAdmins to track attempted break-ins. For example, in February of 1994, co-author Michael Rustad learned through an audit trail that an unknown hacker had attempted to break into his "punitive damages in products liability" database 134 times over a period of three days. Audit controls record every attempted log on and track who signs on when and to which files. Judith Silver, *Routine Workouts Keep VA Security Tight*, GOV'T COMPUTER NEWS, Aug. 8, 1994, at 71.

54. The other main tenet of network security, survivability/availability, is not addressed in this article. "Survivability" refers to the ability to maintain or restore hardware, software and data integrity in event of electronic or natural disaster. "Availability" refers to the consistency and continuity of network functioning.

specifications for C2⁵⁵ security classification.⁵⁶ However, these systems comprise only a small part of the Internet's backbone.

4. LOCAL AREA NETWORK

Network security may be compromised within a LAN. Readers will find words like "network," "computer system," and "LAN" used seemingly interchangeably with "Internet." Generally these terms have separate meanings. In the world of electronic-data security, however, they can be used to refer to computers potentially at risk from intrusion by other, remote computers by virtue of their interconnectedness. Obviously, if a computer or LAN has no connection to the Internet, it is not at risk from Internet hackers. Additionally, if a computer is simply a "stand-alone" computer—it has no connection to a LAN or modem or the Internet—it cannot be at risk from a remote computer. However, a computer connected to a LAN can potentially be hacked into remotely—by or from *any other computer connected to or able to connect to the LAN*. This is the essence of remote intrusion.

The most important protection measure is to restrict physical access to the LAN's server computer to trusted personnel to prevent potential in-house hacking. In addition, LAN O/Ss can be "secure" or "insecure," depending on their hardware, software and configuration. The government certifies federal agencies' operating systems as secure if they meet the standards for C2 security classification.⁵⁷ Currently,

55. The D to A1 rating system was designed by the NCSC, a division of the National Security Agency (NSA), based on a collection of 36 color-coded books known as the "Rainbow Series" (including the widely-referenced "Orange Book"). Under the 1987 Computer Security Act, C2 ("Controlled Access Protection") is the minimum rating federal agencies must comply with to protect sensitive but unclassified information. All hardware and software on the system, including security features, must periodically be tested to ensure proper functioning. Files can be shared, but file access must be controlled, and only authorized personnel may assign user rights. User identification and authentication is required, data must be protected from unauthorized users, and the computer system should protect itself from outside tampering. Accountability is stressed, requiring a detailed audit trail and logging. See Susan Biagi, *How the Government Looks at Security*, STACKS: THE NETWORK J., Dec. 1994, at 37.

The NSA has responsibility for classified national security issues, while the National Institute of Standards & Technology is responsible for non-classified information. Their guidelines are two of only a few published standards on computer system security, and commercial-sector standards are derived therefrom. *Id.*

56. Bob Melford, "Six-0" For Security and Things That Take Six Years, DIGITAL NEWS & REV., Sept. 27, 1993, at 11.

57. Cf. Roger Addelson, *Making Your Customer's Network Secure*, STACKS: THE NETWORK J., Dec. 1994, at 27. For an explanation of what constitutes C2 compliance, see *supra* note 55.

NetWare 4.x, Windows NT Server, Trusted Network Computing Environment and Cordant's Assure are C2 certified.⁵⁸

Individual work station security is also related to LAN security because workstations can be used as unauthorized ports of entry. Disk, screen and keyboard locking mechanisms can be used to prevent unauthorized access when employees are away from their computers. In addition, certain programs prevent unauthorized alteration of configuration and startup files (e.g. CONFIG.SYS and AUTOEXEC.BAT) and/or notify SysAdmins of any attempts to change program initiation (i.e., authorization specification) files. Finally, armoring products either prevent computer-booting through the floppy drive where password security could be bypassed or prevent resetting of computer clocks to make former passwords or SuperUser access retroactive.⁵⁹ Fischer International Systems Corp. makes a suite of products which performs these and other protective functions.⁶⁰

Client computers and LANs which have modems are also vulnerable to external intrusion from outside the local network. A common, and effective, method of preventing this type of unauthorized entry employs a "call-back" protocol. An authorized user who wishes to dial in and use an office computer dials up the computer via its modem. The computer is programmed to allow remote use from only certain, pre-authorized phone numbers. Upon receiving the call-in, the computer terminates the connection, checks the number dialed from against its list of authorized numbers, and calls the user's computer back if the number is an authorized one. When the connection is reestablished, the user must log in and successfully complete the rest of the user identification and authentication challenges in order to initiate the remote session with the computer.

5. FIREWALLS

The Pentagon has 650,000 terminals and work stations; the military has 10,000 local computer networks and 100 long-distance computer networks. The Pentagon currently experiences an average of two hacker attacks per day, "more than double the rate of 255 a year in 1994."⁶¹ Intruders have stolen, altered and even erased Pentagon

58. *Id.*

59. See Horace Labadie, *Digital Crime Watch: Developing an Effective Security System*, COMPUTER SHOPPER, Mar. 1994, at 594.

60. *Id.*

61. John J. Fialka, *Pentagon Studies Art of 'Information Warfare' To Reduce Its Systems' Vulnerability to Hackers*, WALL ST. J., July 3, 1995, at A20.

records.⁶² Robert Ayers, chief of the Defense Information Systems Agency's (DISA) information warfare division, acknowledges that the Pentagon's electronic infrastructure is "not safe and secure."⁶³

The Department of Defense (DOD) developed firewalls for computers and networks in the mid-1980s in order to prevent access to, and leaking of, classified documents.⁶⁴ Firewalls create a shell of protection between a network and possible intruders.⁶⁵ Although they are commonly used to restrict information from exiting or entering a firm's computer or LAN via a modem, firewalls are increasingly being designed and integrated into routers/gateways in order to regulate the flow of information between a LAN and the Internet.⁶⁶ The firewall typically sits on the router and functions by filtering all the electronic data packets sent to it from the LAN and the outside connection.⁶⁷ Only verified electronic data packets are passed on by the firewall's packet filter, assuming the firewall is properly configured. For example, a firewall may be configured to accept (and process) only e-mail type communications data-packets and to accept mail for only a particular set of addressees. In such a case, an intruder attempting to initiate a file-transfer request would be thwarted, as the firewall would not recognize the communications protocol and would thus reject it. In fact, without the proper server program on the host computer, the computer would have no way of responding to such a request.

Vendors offer a wide array of firewalls to provide protection to Internet routers/gateways.⁶⁸ For example, Network Systems markets

62. Bernstein, *supra* note 12, at 49.

63. Munro, *supra* note 23, at C3.

64. Gary H. Anthes, *Hackers Stay a Step Ahead*, COMPUTERWORLD, Oct. 17, 1994, at 14.

65. The purpose of a firewall is to protect sensitive information. Mass-marketed firewall software products include FireWall-1, sold by CheckPoint Software Technology Inc. of Lexington, Massachusetts. FireWall-1 is installed like any other mass-marketed, pre-packaged software without any customized modifications. See generally Streeter, *supra* note 4, at 58. Commercial entities will frequently design their own firewall using an Internet security consultant. Network managers will hire security consultants to design not only firewalls but also network security policies for firms. *Id.*

66. Firewalls for UNIX-based software gateways are increasingly being designed to perform packet filtering. Firewalls are usually part of a larger network security policy employing other protection such as password protection, data encryption and workstation security. *Id.*

67. Routers attached directly to the Internet will use "packet filters." "Packet filters are essentially rule-based programs that instruct a router to accept only certain types of traffic from specified network addresses." Ted Doty, *The Whole Truth About Network Security*, DATA COMM., Nov. 1994, at 150.

68. Some users also employ public-domain firewall tools such as SOCKS. Streeter, *supra* note 4, at 58.

BorderGuard for the protection of remote sites. Another product employs proxies, which are "slimmed-down versions of applications that are open to outside users and serve to protect the 'real' application behind the firewall from bugs."⁶⁹ IBM's "NetSP Gateway" enforces network access rights based on user-determined rules. It also takes action if hacking is suspected based upon an analysis of address pairs and requested services.⁷⁰ Harris Corp. makes a computer safeguard called CyberGuard Firewall, which places a computer between a company's LAN and its outside connections.⁷¹ Trusted Information Systems, Inc. developed Gauntlet, a firewall based on Pentium hardware, using a modified version of Unix.⁷² Firewall technology has evolved considerably in recent years and now provides significant protection against the unwanted inflow or outflow of digital data.

6. PASSWORDS

Passwords were one of the earliest security "devices" developed in the mainframe environment to keep out intruders. Passwords have been less than successful in thwarting security breaches in the LAN environment because of cultural attitudes toward their use and dissemination. A commentator illustrated the lackadaisical attitude toward passwords in a recent demonstration at a conference. Posing as a computer room operator, the security expert simply called the switchboard operator of the local telephone company. The operator willingly provided the impostor with a "critical, top-secret password" granting access to a database of the names and addresses of all of its customers, the "crown jewels" of the telephone company.⁷³ In these cases, the breach does not occur across the Internet, but rather through socially-engineered dial-in access. This type of low-tech hacking is an area where telephone hackers, known as "phrEakers" or "phrackers," have been able to wreak havoc with company computers and telephone accounts.

Other breaches occur via the Internet due to careless password security. The British hacker Paul Bedworth was able to enter

⁶⁹. Joanie Wexler, *Users Send Out an SOS to Internet Providers*, NETWORK WORLD, Feb. 13, 1995, at 37.

⁷⁰. See *id.*

⁷¹. Frank Ruiz, *ECl to Build E-Mail Security Chip for U.S.*, TAMPA TRIBUNE, June 8, 1995, at Business and Finance 1.

⁷². Knowles, *supra* note 30, at 14.

⁷³. Susan Watts, *The BT Hacker Scandal: BT 'Flouted its Own Advice to Government,' Consultants Are Fighting a Losing Battle to Persuade Firms to Protect Their Computer Systems*, THE INDEPENDENT, Nov. 25, 1994, at 3.

numerous government and company computers because they were protected only by the password of the installing engineer or another simple default.⁷⁴ It is estimated that "over half of the passwords in use are said to be the first names of spouses and children, birthday and anniversary dates, and the names of super-heroes."⁷⁵ Passwords such as these are highly susceptible to security breach because a hacker (either a company insider or a remote hacker using the Internet or dial-in access) need only run a hacker dictionary program against the target computer in order to learn the password and thereby access the computer itself.

Hacker dictionary programs operate by trying every word in the dictionary (including variants of words and names) until a password match is found. The shorter the password, the faster it will be cracked. Given the comprehensiveness of these dictionary programs and high speed of computers, common passwords can be broken within minutes or hours. If the vulnerable password is on a router/gateway computer, then the company is making its system vulnerable not only to insiders, but to Internet hackers as well. Fortunately, even a minimalist security program can detect such attempts and set off an alarm. In addition, increasingly effective password-protection schemes are available for implementation. These methods include: "pass-phrases," as opposed to mere pass-words; two-factor identification, which requires inserting a card or "token" belonging to the user along with inputting the proper password; dynamic synchronized password schemes which change the password in both the host and the user token every few seconds; and software-token-based challenge-response systems which use encryption to ensure all transactions are secure.⁷⁶ An example of an advanced password product is one which combines two-factor identification with dynamic synchronization. The password on the synchronized card changes every thirty to sixty seconds, and thus is good only for the duration of a single log-on session.⁷⁷ More secure—and expensive—methods of authenticating user identity are also proliferating.⁷⁸ These advanced methods include verification by retinal scanning,

74. *Id.*

75. Eric H. Steele, *Software Review: Security*, 5 COMPUTER COUNSEL 39 (Aug. 1993).

76. For a description of these and other password security schemes, see Winn Schwartau, *New Keys to Network Security*, INFO WORLD, May 15, 1995, at 51.

77. This smartcard is called SecurId and is manufactured by Security Dynamics, Inc., of Cambridge, Massachusetts. Another smartcard vendor is Enigma Logic, Inc., which produces a product called Safeword. Tom McCusker, *Take Control of Remote Access*, *Network Security Measures*, DATAMATION, Apr. 1, 1994, at 62.

78. Encryption may be used to protect passwords and data, and to verify communications.

fingerprint identification, signature recognition, voice recognition and biometric recognition, which is based on the unique way each user has of inputting her password or pass-phrase.⁷⁹

Even a computer defended with state-of-the-art security will not remain impregnable for long if no on-going efforts are directed toward security. High-tech hackers continually attempt to find new means of obtaining unauthorized access to computer systems. Like automobile anti-theft devices, computer, network and Internet security devices become vulnerable to breach over time. Steps must be taken continually to stay ahead of malefactors' resourcefulness. One recent hacker innovation, known as "spoofing," has proven successful against systems. This technique attempts to access otherwise secure systems by breaking the code words on one computer in a network, then impersonating the "friendly" machine to bypass the defenses of others.⁸⁰ To avoid this risk, SysAdmins should implement programs which adopt a norm of mutual suspicion and demand more thorough authentication.

7. ENCRYPTION

Encryption refers to any algorithm applied to a digital message which scrambles the plain text message, rendering it meaningless to anyone who does not have the key to decrypt the message. The federal government has used Data Encryption Standard (DES),⁸¹ a 56-bit, single key encryption technology, since the mid-1970s for its sensitive, but not classified, information.⁸²

One network security firm makes use of the International Data Encryption Algorithm, the DES and DES III algorithms.⁸³ The firm employ(s) a complex set of software services to connect a secured, corporate network to an unsecured network, such as the Internet. They can be configured to control access, authenticate users, hide some or all of a corporate network to the public and protect live corporate data by permitting access to only parts of applications.⁸⁴

79. Schwartau, *supra* note 76, at 51.

80. See generally RUSSELL L. BRAND, *COPING WITH THE THREAT OF COMPUTER SECURITY INCIDENTS: A PRIMER FROM PREVENTION THROUGH RECOVERY* (1990) (provides simple and cost-effective methods for preventing computer security problems and for incident handling and recovery. Available in USENET newsgroup comp.security.misc).

81. *The Data Encryption Standard*, in FEDERAL INFORMATION PROCESSING STANDARD 73 (1970).

82. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 736 (1995).

83. Roberts, *Network Systems*, *supra* note 30, at 1.

84. Wexler, *supra* note 69, at 37.

Encryption technology is expected to significantly advance the security of on-line commerce. However, encryption technology will not remain secure if the technology becomes outdated or compromised. For instance, the National Institute of Standards & Technology (NIST), while re-authorizing the government's use of DES in 1993, simultaneously indicated the approaching end of its usefulness.⁸⁵ Due to the yearly near-doubling of computer speed and power, breaking an encryption key through "brute force" takes less and less time.

Until recently, all of the most secure systems used single key algorithms.⁸⁶ The new public key/private key encryption technology, such as that incorporated into RSA⁸⁷ encryption technology, is being hailed as a practical solution for secure Internet transactions.⁸⁸ RSA is marketed by RSA Data Security of Redwood City, California, and it has become the de facto encryption industry standard.⁸⁹ It is built into current or planned O/Ss for Microsoft, Apple, Sun and Novell.⁹⁰ It is also used in secure telephones, Ethernet network cards and smart cards.⁹¹

RSA's public key/private key encryption technology⁹² has two advantages over previous encryption technologies.⁹³ First, the addition of the private key, which is known only to the sender, adds an additional layer of security. With DES, each party had to simultaneously know the secret key. With RSA, the public key is published widely but the private key is held by only one person. Assuming the private key is not disclosed, the result is message confidentiality and transmission security. Thus, when the sender

85. Froomkin, *supra* note 82, at 738 n.120.

86. See BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 273-74 (1994). See generally *id.* at 219-320 (providing extensive information on block cipher encryption schemes such as DES and public key encryption schemes such as RSA).

87. "RSA" stands for the names of its MIT inventors: Ron Rivest, Adi Shamir and Leonard Adleman. The RSA algorithm was introduced in 1978. SCHNEIER, *supra* note 86, at 281-82.

88. Liu, *supra* note 2.

89. See RSA'S FREQUENTLY ASKED QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY 8 available on RSA's Web site: "http://www.rsa.com/rsllabs/faq/faq_rsa.html#rsa.1" (hereinafter RSAFAQ).

90. *Id.*

91. *Id.*

92. Public key cryptography was invented in 1975 when Whitfield Diffie published an article conceptualizing it with the assistance of Martin Hellman, a Stanford University computer scientist. RSA algorithms can also be found in Phil Zimmerman's Internet-distributed program entitled "Pretty Good Privacy" (PGP). Public key cryptography is likely to be popular in the Privacy Enhanced Mail program (PEM), as well.

93. See generally EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 30 (1994) (explaining public key encryption).

("A") transmits a message using the recipient's ("B") *public key*, only the proper recipient, B, has the *private key* necessary to decode it. Conversely, when sender A transmits a message encoded with her own *private key*, any recipient with sender A's *public key* can decode it, but the *private key* acts as a digital signature, authenticating that A is in fact the sender and that the message has not been altered. Barring what is known as a "man in the middle" security breach, recipient B knows the message could only have been sent by A.

While public key processing has the disadvantage of being about 100-times slower in software and 1,000 times slower in hardware than DES,⁹⁴ various methods are already circulating to mitigate this shortcoming. One solution is to use RSA primarily to transmit brief messages. For longer messages, RSA encryption can be used to send the recipient a one-time single key encryption scheme, which then can be used to send the subsequent long message.⁹⁵ Since the single key encryption scheme is used only one time, the security of the transmission is not compromised. A third method, known as "RSA digital envelope," combines DES and RSA as follows: "[F]irst the message is encrypted with a random DES key, and then, before being sent over an insecure communications channel, the DES key is encrypted with RSA. Together, the DES-encrypted message and the RSA-encrypted message are sent."⁹⁶

RSA's second major advantage is that its keys are functions of a pair of extremely long prime numbers for which no factoring algorithm is currently known.⁹⁷ If hackers could discover a factoring algorithm or other cryptanalysis scheme for RSA, they would have a "shortcut" to breaking RSA keys.⁹⁸ Until and unless a factoring algorithm is discovered, however, hackers are reduced to trying to break keys by "brute force." This entails systematically trying every combination of numbers, letters, or symbols which conceivably could comprise the key until the proper combination is found.

Michael Froomkin describes the mammoth resources needed to crack a 129-digit RSA key by brute force:

A group of computer scientists and mathematicians recently used the Internet to harness computer time donated by 600 volunteers. Using a total of about 5,000 MIPS-years [approximately the equivalent of the power of 33 100 Mhz Pentiums running for a year] of processing time to make 100

94. SCHNEIER, *supra* note 86, at 285.

95. *Id.*

96. RSAFAQ, *supra* note 89.

97. SCHNEIER, *supra* note 86, at 282.

98. *Id.* at 284.

quadrillion calculations over an eight month period, the group solved a problem equal in complexity to breaking a 129-digit RSA key.⁹⁹

Michael Froomkin notes that the increasing potential of parallel processing "might make it possible to break even a 512-bit [64-digit] key at a cost . . . well within the means of the poorest government."¹⁰⁰ While this may be so, common sense dictates that any foreign governments attempting to crack RSA keys will direct their efforts at high-level federal offices or corporate institutions. In addition, while governments may have the resources to crack a 64-digit RSA key, most RSA keys are two to three times longer than that. The longer the key, the greater the security. Entities with very high security needs can use long keys and combine them with additional measures to assure security. The average American's on-line commerce should suffer no risk from foreign intrusion because the cost so outweighs the gain as to make it impractical.

With regard to private hackers, it is doubtful that even the most determined ones will be able to marshal the necessary resources to crack 64-digit RSA keys. While a student at France's Ecole Polytechnique in Paris cracked an RSA-based key on Netscape's browser in August of 1995 by running a network of 120 computers for eight days,¹⁰¹ the keys were only five digits or less in length.¹⁰² In addition, the "serious security flaw" discovered in Netscape's domestic browser in September of 1995 by two computer science students at the University of California at Berkeley was due to Netscape's flawed random-number generating system, not the RSA key itself.¹⁰³ The company announced it would incorporate a more complex coding formula plus a coding string ten times longer than its predecessor.¹⁰⁴ One industry expert markets encryption systems using 170-digit RSA keys and flatly asserts they are "unbreakable."¹⁰⁵

99. Froomkin, *supra* note 82, at 740.

100. *Id.* at 888. Professor Froomkin cites an estimate that a 512-bit [64 digit] key can be broken with approximately \$8.2 million worth of equipment. *Id.* at 775.

101. John Markoff, *Software Security Flaw Put Shoppers on Internet at Risk*, N.Y. TIMES, Sept. 19, 1995, at A1.

102. It takes eight "bits" of information to create a single digit, or character, in computer language. Although the Clinton Administration is considering allowing the export of encryption code of up 64 bits, the maximum-length encryption code currently exportable is 40-bit. Forty bits of information would produce a maximum of five digits or characters. *New Policy Proposed on Software Protection*, ATLANTA J. & CONST., Aug. 20, 1995, at 6.

103. Markoff, *supra* note 101, at A1.

104. The coding string will be essentially a 50-digit RSA key. *Id.*

105. Daniel M. Federman, President, Premenos, *Protecting Enterprise Information in the Digital Age: Encryption, Digital Telephony, Privacy and Security*, Presentation

Given the growing recognition of the security assurance provided by public key cryptography, major corporations and institutions are forging ahead with schemes for on-line commerce. The latest version of Netscape's World Wide Web browser supports RSA encryption, which is designed to facilitate secure Internet transactions. MasterCard has been working with Netscape Communications Corp. to effectuate secure electronic commerce.¹⁰⁶ Visa International, Inc. has undertaken a joint venture with Microsoft Corp. to develop a software program that will allow customers to make secure credit card payments over the Internet by making use of passwords.¹⁰⁷ Europay, Europe's largest credit card company, initiated a joint venture with International Business Machines Corp. in June to develop a scheme for conducting secure business over the Internet.¹⁰⁸

8. DIGITAL SIGNATURES

"Digital signatures," designed to insure against falsification or alteration,¹⁰⁹ are also becoming part of the accepted legal infrastructure in the information security field. This technology, which employs cryptography to secure information, also provides a

at the American Bar Association Section of Science & Technology Annual Meeting (Aug. 7, 1995).

106. *Visa, MasterCard Plan Internet Venture*, L.A. TIMES, June 23, 1995, at D3.

107. *Id.*

108. *Id.*

109. The ABA Science and Technology Section guidelines describe digital signatures as being

created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. For digital signatures, two different keys are generally used: one for creating a digital signature or transforming data into seemingly unintelligible form, a process often termed "encryption," and another key for verifying a digital signature or returning the message to its original form, a process often termed "decryption."

Computer equipment and software utilizing two such keys is often termed an "asymmetric cryptosystem." The keys of an asymmetric cryptosystem for digital signatures are termed the *private key*, which is known only to the signer and used to create the digital signature, and the *public key*, which is ordinarily more widely known and is used to verify the digital signature. A recipient must have the corresponding public key in order to verify that a digital signature is the signer's. If many people need to verify the signer's digital signatures, the public key must either be distributed to all of them or published in an on-line repository or directory where they can easily obtain it.

Information Security Committee, American Bar Association, DIGITAL SIGNATURE GUIDELINES WITH MODEL LEGISLATION 22 (Provisional Draft, July 26, 1995).

means of identifying the sender.¹¹⁰ The goals of an effective digital signature system are to achieve signer authentication, document authentication, affirmative acts signifying a signature and efficiency.¹¹¹ The ABA "Digital Signature Guidelines" seek to: 1) minimize the incidence of electronic forgeries; 2) enable and foster the reliable authentication of documents in computer form; 3) facilitate commerce by means of computerized communication; and 4) give legal effect to the general import of the technical standards for authentication of computerized messages.¹¹² Digital signatures, like encryption technology in general, secure electronic transactions from point of origin to point of receipt.

9. THE ODYSSEY OF THE GOVERNMENT'S CLIPPER CHIP

The National Security Agency (NSA) designed the so-called "Clipper Chip," with the single-key based algorithm SKIPJACK, to defeat cellular-based security breaches.¹¹³ Its purpose was to prevent private parties from using encrypted cellular-based communications for illegal purposes.¹¹⁴ The original plan for the Clipper Chip entailed a tradeoff: the government would provide the private sector with encryption technology certified by the NSA as unbreakable for years to come, and recipients would allow government agencies to hold their secret keys in escrow.¹¹⁵ The keys would be divided into two parts and housed with escrow agents at two different government agencies, the Treasury Department's Automated Systems Division and the Commerce Department's NIST, both executive-branch offices.¹¹⁶ The escrowed keys could only be obtained for a given purpose by law enforcement officers exercising legal warrants.¹¹⁷ The secret keys would allow law enforcement to decode Clipper-encrypted

110. *Id.* at 31.

111. *Id.* at 20-21.

112. *Id.* at 33.

113. *Privacy Issues in the Telecommunications Industry: Testimony Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 103d Cong., 2d Sess. (1994) (statement of Stephen T. Walker, President, Trusted Information Systems).

114. See Stephanie Stahl (with Mary E. Thyfault), *About Face on Clipper—Privacy Advocates Draw Conflicting Conclusions on Encryption Policy*, INFO. WK., Aug. 8, 1994, at 24.

115. Froomkin, *supra* note 82, at 715-16.

116. See Rochelle Garner, *Clipper's Hidden Agenda*, OPEN COMPUTING, Aug. 1994, at 54.

117. *Id.* at 54

communications. A similar system was envisioned with regard to data-based information utilizing the Capstone algorithm.¹¹⁸

Clipper and Capstone have stirred considerable controversy. They are opposed by civil libertarians who view the government's ability to break strong cryptography at will as the predecessor of Big Brother.¹¹⁹ Others oppose them on constitutional bases.¹²⁰ Those with commercial interests fear that a product the U.S. government can tap into "at will" will be anti-competitive on foreign markets, as well as at home.¹²¹ Global marketeers maintain that the true agenda of Clipper/Capstone is to ensure that the NSA retains control over exports.¹²²

On the other hand, at least one nationally respected security analyst argues that not only law enforcement officials, but also regulatory agencies such as the Securities and Exchange Commission, the Food and Drug Administration and the Atomic Energy Commission should have access to the keys: "All [such agencies] must have the capability to eavesdrop on the industries they watch over under hostile circumstances. Because if we have powerful cryptography freely available to our citizens, and the government does not have an eavesdropping capability, our democracy will be destroyed."¹²³

Given the controversy and opposition, it is unlikely that Clipper and Capstone will succeed in their original form. A representative of the Federal Bureau of Investigation reports that progress is being made with the Clipper initiative.¹²⁴ The federal government has agreed to allow Clipper keys to be escrowed with private entities rather than governmental agencies. Foreign governments are more receptive to the idea since they share with the U.S. the objective of deterring terrorists.¹²⁵

118. Allan McDonald, Federal Bureau of Investigation, Protecting Enterprise Information in the Digital Age: Digital Telephony, Privacy and Security, Presentation at the American Bar Association Section of Science & Technology Annual Meeting (Aug. 7, 1995); see also Froomkin, *supra* note 82, at 715-16 n.16.

119. See Garner, *supra* note 116, at 51 (describing the Clipper Chip controversy).

120. See Froomkin, *supra* note 82, at 810 (discussing personal privacy, freedom of association, free speech, unreasonable search and seizure, and potential self-incrimination issues in the context of a governmental mandatory encryption key escrow scheme, which some commentators believe to be implicit in the Clipper initiative).

121. Garner, *supra* note 116, at 52.

122. *Id.*

123. *Id.* at 52 (quoting Donn Parker, program manager of information and security, SRI International, Menlo Park, Cal.).

124. McDonald, *supra* note 118.

125. *Id.*

Meanwhile, the government has legitimated public/private key encryption technology. This is apparent in the recent establishment by the U.S. General Services Administration (GSA) and the DOD of an office whose task is to implement the "highest standards" of security within the government's electronic system by implementing a "public key encryption infrastructure and the widespread capability to handle secure digital signatures."¹²⁶

10. AUTHENTICATION OF ELECTRONIC COMMERCIAL TRANSACTIONS

The optimism that the security problem can be solved has led to recent exponential growth of electronic commerce.¹²⁷ For example, "ExpressNet," recently developed by the partnership of American Express and America Online, permits consumers to pay bills and download their billing histories along with a history of recent transactions directly into their computer's financial-management software.¹²⁸

Banking on the Internet will soon flourish in a secure environment thanks to joint ventures between MasterCard International and Netscape Communications Corp., and between Visa International and Microsoft.¹²⁹ Another firm has introduced a product which purportedly enables organizations to exchange information in total confidentiality across all types of private and public access data networks, including the Internet.¹³⁰

Consumers also may now access their credit cards from "electronic wallets" displayed on their computer screens and consummate financial transactions without having to set up special accounts with businesses in advance.¹³¹ Many companies are racing to introduce digital money, or "E-Cash" systems; Citicorp is developing an "entire infrastructure for using electronic money to be issued by Citicorp and

126. Kennedy Maize, *GSA & Department of Defense Open Information Security Offices*, NEWSBYTES, May 24, 1995, available in USENET Newsgroup clari.nb.govt., Article 707 (emphasis added).

127. See, e.g., *Technology Briefs*, THE PLAIN DEALER, Apr. 9, 1995, at 4l.

128. Jared Sandberg, *American Express Goes On-Line for Card Holders*, WALL ST. J., Jan. 30, 1995, at A3.

129. *Id.*

130. See, e.g., Micahel Csenger, *NSC Unveils Next-Generation Router/ATM Campus Switch*, NETWORK WORLD, Nov. 14, 1994, at 3; see also, *ATM: Network Systems Corp. Introduces Networks-On-Demand on New Enterprise Routing Switch: Single Platform Combines Routing & Switching With ATM Connectivity*, EDGE, Nov. 14, 1995.

131. *Technology Briefs*, *supra* note 127, at 4l.

other banks."¹³² Even an automated clearing house for mutual funds is slated for the Internet by Galt Technologies' "NETworth" service.¹³³

11. COMBATING THE ENEMY WITHIN ORGANIZATIONS

While encryption seems to be providing a solution to the problem of insecure Internet transactions, many firms are still failing to take adequate internal security measures to protect against computer security breaches by their employees. Ernst & Young's study of 1,271 companies concluded that slightly more than a third of firms perceived their senior management as being only slightly concerned with information security.¹³⁴ Eight percent indicated that their management perceived security issues to be not important at all.¹³⁵

One in four companies have sustained losses from network security breaches in the past two years, many of which were committed by disgruntled employees or ex-employees.¹³⁶ For example, a bank officer attempted to embezzle \$15.1 million by electronically transferring funds into his own Swiss account.¹³⁷ An ex-employee at another company was allegedly caught, three months after being fired, in the act of downloading proprietary software from the company's computer. A password she had shared with five other employees had not been changed after her dismissal. She was able to spend eighteen hours copying programs before a phone trace led to her arrest.¹³⁸

Detection of internal misappropriation is a much more complicated issue than locking the doors at night; however, effective deterrence is attainable through implementation of adequate security measures. It is recommended that, in the event of a hostile employee termination, an escort should accompany the ex-employee while he cleans out his office and transfers any security codes back to the firm.¹³⁹ Any security code that was in the hand of a disgruntled ex-employee should be presumed compromised. Passwords and other

132. Kelley Holland & Amy Cortese, *The Future of Money: E-Cash Could Transform the World's Financial Life*, BUS. WK., June 12, 1995, at 66.

133. *Cyberspace Comes to Mutual Funds in Next Wave of "Home Banking,"* BANK MUTUAL FUND REP., May 31, 1995, at 1.

134. Jared Sandberg, *Losses Linked to Lax Security of Computers*, WALL ST. J., Nov. 18, 1994, at B4.

135. Thirty-four percent of respondents believed that information security was viewed by their managers as only "somewhat important." *Id.*

136. Addelson, *supra* note 57, at 27.

137. *Id.*

138. *Id.*

139. *Protecting Your Data When Firing Employees: A Sensible Precaution*, ROCKY MOUNTAIN NEWS, Dec. 3, 1994, at A71.

security devices must be changed within a few hours. Surrendering of access codes should have the same status as returning keys, credit cards and building access credentials.¹⁴⁰ An essential part of changing access codes is keeping a good record of all access by the ex-employee.

In-house computer system security can be rendered meaningless if passwords are written down, known to others, shared, easily guessed, or subjected to hacker dictionary programs. The insider-practice of "shoulder-surfing" to steal the passwords of users who have broader access privileges represents a potentially greater threat to computer system security than outside hackers.¹⁴¹ Current password protocols are acknowledged to be "often inadequate to prevent unauthorized access to a computer system."¹⁴² The current overwhelming ignorance and indifference toward password security in companies constitutes one of the greatest threats to computer systems' security. Yet it is a self-inflicted wound. The patient can cure himself quite easily with a little effort and minimal resources. Informal password protocols are already available, and tailored formal versions can be implemented within companies with relative ease. Although password security and adequate employee-access security require implementing special security policies, their proper implementation should virtually eliminate the occurrence of computer break-ins by insiders.

B. The Internet/Network Security Industry

Prior to the mass-marketing of the Internet, computer system security was essentially lore developed and shared by SysAdmins who communicated electronically on newsgroups dedicated primarily to discussion of Unix-based systems. This dialogue about Unix security loopholes and remedies provided the basis for today's network security industry. With the PC revolution and advent of the National Information Infrastructure, companies and organizations began to recognize the security risks inherent in their in-house computer systems. They called in these Unix "experts" to analyze risk and recommend and implement security solutions. The commercial network security industry was born.

Commercially, the industry is still young. There are no nationally-recognized standards for classifying persons as "network

140. Steele, *supra* note 75, at 35.

141. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change: Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 311-12 (1993).

142. *Id.* at 311.

security consultants,"¹⁴³ and such consultants have not been deemed by courts to comprise a "profession."¹⁴⁴ Nevertheless, the emergent industry has rapidly progressed from providing pure consulting services to companies with Unix mainframes on an ad-hoc basis to developing a number of countermeasures to mitigate the danger of unauthorized access, theft, or damage to a computer's intangible electronic data. Like home break-ins, computer intrusion can be combated by a spectrum of methods and products. The various components and considerations discussed in the previous part can be applied singly or in combination to achieve the desired level of safety from Internet intrusions as well as in-house hackers. For example, company employees who encrypt sensitive e-mail communications are protecting the company against in-house security breaches as well as Internet hackers. In these cases, "network" security truly is synonymous with "Internet" security. Other countermeasures are designed more specifically to thwart either Internet or in-house security breaches.

The majority of network security solutions are like the intangible electronic data they are designed to protect in that they are computer programs. Since the 1980 amendment to the Copyright Act, software has been specifically recognized as copyrightable.¹⁴⁵ This protection has had a significant impact on the industry by introducing intellectual property considerations. Complicating the arrangement is the fact that software programs are not sold; they are licensed. This problem will be discussed in part IV. Not all security solutions, however, are software. Many are combination software/hardware solutions. Some are pure intangibles, and others pure personnel policy. Some consist of security consultant services leading to personnel or SysAdmin protocol recommendations. The major categories of

143. Major players in the computer industry support their own certification programs, which can provide some guidance in assessing a proclaimed network security professional's competence. For example, Microsoft provides a certificate to those individuals who pass Microsoft's exam on Windows NT. Windows NT is Microsoft's renowned operating system for networks which are C2 compliant. A customer shopping for a network security professional would thus have fair assurance that such a certified individual would have the expertise to install, configure and maintain a Windows NT server and network in a secure operating manner. See BECOMING A MICROSOFT CERTIFIED PROFESSIONAL, available at "http://www.microsoft.com/moli/advising_building/certifications/introduction-to-certification.html" on the World Wide Web.

144. See *infra* note 176 and accompanying text.

145. H.R. REP. NO. 1307, 96th Cong., 2d Sess. 23 (1980), reprinted in 1980 U.S.C.A.N. 6460, 6482; 17 U.S.C. § 101 (definitions), 109 (limitation on exclusive rights of copyright owner), 117 (special provision providing for noninfringement of certain uses of computer programs).

commercial security solutions that have developed to date are outlined below.

1. MASS-MARKETED NETWORK / INTERNET SECURITY PRODUCTS

Most security products are software, sets of instructions housed on diskette or CD-ROM that are designed to perform designated security functions. The simplest examples are programs which perform a single primary security function, such as anti-virus programs. Prime examples are Norton Anti-Virus and McAfee Anti-Virus. More sophisticated programs offering more comprehensive protection are also available as mass-marketed software products. For example, Norton's Disklock can be used on a single computer or a network to restrict access to hard drives, directories and files to authorized users only. Like dead bolts and window bars for the home, software security products can be purchased and installed by the consumer to deter specific threats.

2. OWNER-DISTRIBUTED SECURITY PRODUCTS

A significant portion of network security products are not mass-marketed, but are distributed by the developers themselves and/or their authorized representatives. Security products within this category include firewalls, as well as hardware and software access control products, such as Security Dynamics Technologies, Inc.'s Ace/Server and ACM, respectively,¹⁴⁶ and properly configured network servers, such as Cylink Corp.'s SecureManager.¹⁴⁷ Owner-distributed products are typically more complex than mass-marketed products. They are frequently a combination of hardware and software, and require more detailed installation and administration procedures. Despite their complexity, the trend in the industry is to market these products without a "services" component. Thus, the burden is on the customer to install and maintain the hardware and software correctly. The contract in Appendix A, "Example of a Sales and License Agreement of a Network Security Product," typifies this arrangement.

146. *Security Dynamics Expands Internet User Authentication Security*, BUS. WIRE, Sept. 26, 1995. Security Dynamics Technologies, Inc. of Cambridge, Massachusetts has gone even further and linked its two-factor SecurID passcode and its ACE/Server software access control product with Trusted Information Systems' Gauntlet firewall to "deliver a unique combination of undefeatable security with ease-of-use" in protecting networks from unauthorized access via the Internet. *Id.*

147. *Network Security*, NETWORK MANAGEMENT SYSTEMS & STRATEGIES, Sept. 19, 1995.

3. CUSTOMIZED SECURITY

Innovation and proliferation of security products has decreased the likelihood of a "network security professional" being called on to custom-develop a security product or system. In most instances, a security consultant will analyze the vulnerabilities of a system and remedy them with a combination of already-available services, tools and protocols. This is primarily a services transaction, as opposed to a sale or license. For instance, a network security consultant might conduct a security audit of the company's network to discover an improper or inadequate configuration of the network's server computer. The security consultant would then correct the vulnerability by properly configuring the server. Depending on the company's security needs, she might additionally recommend and install various security products, such as a program that requires users to change their passwords every thirty days or a digital notary system. Just as importantly, the consultant might advise the company on the adoption of personnel policies for protection against in-house and Internet hackers.

4. FREWARE AND SHAREWARE SECURITY TECHNOLOGIES

A number of Internet security technologies are pure intangibles. They are neither mass-marketed nor distributed by licensed dealers—they are simply available for downloading from the Internet. For example, a non-commercial version of the PGP encryption scheme was placed on the Internet for free dissemination by its creator, Phil Zimmerman.¹⁴⁸ This is an example of "freeware," software which can be downloaded from the Internet and used indefinitely without incurring any costs.

Security technologies also include "shareware." Like freeware, shareware can be downloaded directly from the Internet. Unlike freeware, it is provided on a trial basis for a limited time only, usually thirty days. Shareware operates on the honor system, allowing a user to "sample" the technology at no charge. If the user then decides to continue using it, she is expected to pay for and register the "product." Technically, nothing prevents a user from continuing to use technology that she has not paid for. However, disseminators of shareware can and do incorporate various payment incentives. For example, shareware technology is often scaled-down in capability from its registered counterpart. Registration entitles a

148. For a description of PGP, see *supra* note 92. For an excellent introduction to PGP and its use, see BACARD, *supra* note 44, at 125.

user to receive the full version, plus free updates and technical support. An example of a shareware security technology is McAfee's Anti-Virus program, which can be downloaded from McAfee's Internet site.¹⁴⁹

Freeware and shareware security technologies can be downloaded and used without the help of an Internet security consultant. Likewise, mass-marketed products that require little more than simple installation and provide menu-driven prompts for proper use do not require an Internet security consultant. Yet, these technologies and products form an important part of the Internet security industry. They are indicative of the manner in which Internet security is being made more readily available, more user-friendly and more seamlessly woven into every aspect of everyday computing. At this stage, network security consultants are still crucial for helping companies connected to the Internet protect their informational treasure troves. To do this, network security professionals employ an ever-increasing and effective complement of Internet security products, tools and protocols.

The basic building blocks of a secure Internet are already in existence and in use. Hardware and operating systems can be rendered reasonably secure when properly maintained and configured by trusted personnel. Network security products, such as self-diagnostic tools and firewalls, are critical to achieving this goal. Other security technologies such as encryption and digital signatures have demonstrated the ability to secure Internet transactions. Vulnerabilities such as weak passwords and unauthorized access can be remedied through several means. These include implementation of appropriate personnel policies, institution of more sophisticated password schemes or products, and installation and use of hacker detection programs. With today's availability of network security products and the use of proper security protocols, Internet security¹⁵⁰ is no longer the unreasonable proposition or "oxymoron" it was in the past.

III. THE QUESTION OF LEGAL STANDARDS FOR INTERNET SECURITY

This part examines liability for Internet security products in light of traditional tort and contract doctrine. As demonstrated in

149. McAfee's address on the World Wide Web is "<http://www.mcafee.com>."

150. Having explained the relationship between network and Internet security, this article hereinafter uses the term "Internet security" to encompass both network and Internet security.

part II of this article, Internet security products are vital to the successful development of the National Information Infrastructure. They are part and parcel of bringing American commerce and business on line. Yet, at present, the law is unclear as to how liability would be allocated in the event of an Internet security breach that results from a security product's failure. The law of computer bulletin boards has been called "a land with no maps and few native guides."¹⁵¹ The same is true of Internet security. This part analyzes results that could be obtained from applying negligence and strict products liability theories, as well as traditional contract theory and Article 2 of the Uniform Commercial Code (U.C.C.), to claims of Internet security breach. We find that each of these traditional doctrines and theories is ill-equipped to deal with the novel issues associated with the emerging security-related technologies.

A. Regulation Under Tort Law

Each episode of the 1940s radio program "The Shadow" commenced with a mysterious voice asking, "Who knows what evil lurks in the minds of men? . . . The Shadow knows."¹⁵² A sinister laugh followed. That laugh is emblematic of the seamier side of the Internet. The anonymity of Cyberspace grants its citizens the freedom to adopt virtual roles and status with impunity. There are no easy methods of punishing and deterring electronic stalkers, converters, defamers and other intentional wrongdoers. The entire purpose of the Internet security field is to offer products and services to counter the dangers of what Anne Branscomb calls "true anonymity in the Network."¹⁵³ Yet it is not clear who should bear the burden of security breaches.

Are Internet security and service providers liable under tort law for security breaches by anonymous Internet wrongdoers? The *Restatement (Second) of Torts* takes the view that any invasion of a legally protected interest, whether based in negligence, strict liability or intentional misconduct, can be punished under tort law.¹⁵⁴

151. Loftus E. Becker, Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted By Others*, 22 CONN. L. REV. 203, 205 (1989).

152. JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE xi (2d ed. 1991) (comparing the loss of privacy due to the government's assembling of data files with the loss of privacy inherent in the concept of an all-knowing Shadow).

153. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1641 (1995) (arguing that anonymity and accountability are conflicting values in Cyberspace).

154. RESTATEMENT (SECOND) OF TORTS § 6 (1965).

The following discussion applies negligence and strict products liability theories to the role of Internet security providers and identifies possible defenses available to them under tort law.

1. LIABILITY FOR NEGLIGENCE

One can be liable for negligence if one's conduct falls below the standard established by law for protecting others against unreasonable risk of harm.¹⁵⁵ In other words, negligence "is a departure from the conduct expected of a reasonably prudent man under like circumstances."¹⁵⁶ In the business context, this principle provides that a company, holding itself out as capable in its business, impliedly represents that it will perform its work with the "diligence ordinarily possessed by well-informed members of the trade or profession."¹⁵⁷

Before tort law can be applied to a new type of conduct, the appropriate standard of care must be established. Common law negligence does not define a level of care for Internet security providers, and ambiguities result when the historical means of establishing such a standard are employed. Moreover, no statute has been enacted to define Internet security standards. The application of negligence doctrine to the business of providing on-line services highlights these open questions and exemplifies why current negligence theory is ill-equipped to deal with Internet security liability.

a. Common Law Negligence

Many questions arise in trying to apply negligence theory to an Internet security breach caused by a failed security device. For instance, would the failure of an Internet security product be held to be like the barrel of flour that fell out of the miller's window and struck the passerby in the classic case of *Byrne v. Boadle*?¹⁵⁸ In *Boadle*, no evidence indicated that the miller was in any way negligent. The

155. *Pence v. Ketchum*, 326 So. 2d 831, 835 (La. 1976).

156. *Id.*

157. *Data Processing Servs., Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314, 319 (Ind. Ct. App. 1986); *see also* *Young v. McKelvey*, 333 S.E.2d 566 (S.C. 1985) (employee expressly or impliedly promising to perform work in a diligent and reasonably skillful manner); *Crank v. Firestone Tire & Rubber Co.*, 692 S.W.2d 397, 400 (Mo. Ct. App. 1985) (company claiming ability to perform work impliedly warrants that the work will be accomplished in a workmanlike manner); *Standard Roofing Co., Inc. v. Ragusa Bros., Inc.*, 338 So. 2d 119, 123 (La. Ct. App. 1976) (roofing company impliedly promises in every contract that work will be performed in a good and workmanlike manner).

158. 2 H. & C. 722, 159 ENG. REP. 299 (1863).

court held that the accident alone was prima facie evidence of negligence. If a hacker bypasses supposedly "hacker-proof" security devices, should the Internet security professional likewise be presumed negligent,¹⁵⁹ or should the plaintiff have the burden of showing that the security provided was unreasonably lax?¹⁶⁰

In addition, should we prefer rules or standards in setting the level of care for Internet security professionals? In the negligence context, *rules* generally prescribe the conduct which a person must follow in particular situations. For instance, motorists in the early twentieth century were required to stop, look and listen at a railroad crossing or be barred from recovery for railroad crossing injuries attributable to the railroad's negligence.¹⁶¹ In contrast, *standards* require only due care in the circumstances. While bright-line rules have the advantage of offering certainty, they lack the flexibility and ability to accommodate social change offered by standards.

Service aspects of Internet security products would most likely be actionable under negligence. In accord with common law negligence theory, the test for the Internet security service provider's exercise of due care would be objective: what care would a reasonable professional exercise under like circumstances?¹⁶² Assuming a

159. For the doctrine of *res ipsa loquitur* to apply, it must be more probable than not that defendant's negligence was the cause of harm. In addition, the defendant must be in exclusive control of the instrument causing harm, and the harm must not have been caused by any voluntary action on the part of the plaintiff. See *Newing v. Cheatham*, 540 P.2d 33 (Cal. 1975). A defendant cannot be held liable on mere conjecture (a computer may crash as result of a virus planted by a third party, but such is only one possible explanation of the unexplained loss of data) or the mere possibility of negligence (plaintiff suffers unfavorable reaction following administration by doctor of anesthetic). Likewise, absent a showing that defendant was in exclusive control, liability will not be imputed. See *Larson v. St. Francis Hotel*, 188 P.2d 513 (Cal. App. 1948) (holding that, because defendant did not have exclusive control over hotel room, liability under *res ipsa loquitur* did not apply to injuries caused by chair falling out of a room in defendant's hotel). Or, if a passenger is injured in a collision of a trolley with a truck, *res ipsa loquitur* will not apply against either the motorman or the truck driver. See William Prosser, *Res Ipsa Loquitur in California*, 37 CAL. L. REV. 183, 184-89 (1949).

160. The answers to these questions cannot be resolved with certainty due to the unique nature of information technologies. However, it would appear that the doctrine of *res ipsa loquitur* would not apply because of the difficulty of proving exclusive control of the dangerous instrumentality (i.e., the Internet security device).

161. *Baltimore & Ohio R.R. Co. v. Goodman*, 275 U.S. 66 (1927); but see *Pokora v. Wabash Ry. Co.*, 292 U.S. 98 (1934) (promoting caution in framing standards that amount to rules of law and specifically limiting the *Baltimore* decision).

162. *Blythe v. Birmingham Water Works Co.*, 156 Eng. Rep. 1046, 1049 (Ex. Ch. 1956) (holding that a public utility was not liable for "a contingency against which no reasonable man can provide").

plaintiff¹⁶³ could show sufficient deviation from the standard of care and resultant damages, a court could find a defendant Internet security services provider liable for damages. However, what would be the measure of the "reasonable professional" in this new profession? There is no currently-defined standard of care for Internet security professionals. Absent this definition, it is unclear how courts would interpret the duty of the "reasonable Internet security professional."

A beginning point for setting the standard of care for Internet security professionals could be to examine what is customary in the Internet security industry.¹⁶⁴ Widely shared norms could be the basis of a negligence lawsuit against an Internet security service provider who deviates from such norms.¹⁶⁵ However, compliance with an industry custom may be considered only the floor, and not the ceiling, in the setting of the standard of care.¹⁶⁶ In the field of Internet security, firms that conform to the most secure practices and comply with the best available technology would clearly satisfy the standard of reasonable care. The difficult question, however, would be, "How good is good enough?" If it is not customary for most firms to do security audits, will a firm that failed to perform such an audit be deemed to have satisfied the standard of reasonable care?

In *The T.J. Hooper*,¹⁶⁷ two tugboats were lost in a storm. The boats might have avoided disaster if they had been equipped with radios to receive the weather reports transmitted twice a day. The defendants defended on the basis that it was not customary to install radios in the boats. Judge Learned Hand rejected the defense of custom as a negligence "safe harbor." He stated:

[I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests . . . Courts must in the end say what is

163. The plaintiff could be a disappointed recipient of such services or a third-party beneficiary. Whether a duty was owed to the third party would likely be determined by the test of reasonable foreseeability: i.e., would an injured third party be within the zone of danger foreseen by the security professional?

164. Usage of trade is always relevant in assessing breaches of warranty under Article 2 of the Uniform Commercial Code. U.C.C. § 1-205 (1990).

165. It has been suggested that the doctrine of *res ipsa loquitur* could be applied to computer vendors, programmers and others participating in the construction of software. See Vincent M. Brannigan & Ruth E. Dayhoff, *Liability for Personal Injuries Caused by Defective Medical Computer Programs*, 7 AM. J.L. & MED. 123, 143 (1981). However, there is no case law on this possible approach to proving computer software negligence.

166. See generally Clarence Morris, *Custom and Negligence*, 42 COLUM. L. REV. 1147 (1942).

167. 60 F.2d 737 (2d Cir. 1932).

required; there are precautions so imperative that even their universal disregard will not excuse their omission.¹⁶⁸

By analogy, Internet security firms that provide lax Internet security may be found to be negligent if a judge finds that there are readily available security protocols or technologies that may reduce excessive and preventable risks of hacker entry.¹⁶⁹ Comparable judgments may be rendered against the companies who practice lax security in their firms, as well. Compliance with industry norms is not necessarily reasonable. Justice Oliver Wendell Holmes stated that "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."¹⁷⁰

Efficiency may serve as a starting point for establishing "what ought to be done." The goal should be to reduce Internet information theft and security breaches to the point where the damages caused by such breaches equal the burden of precaution.¹⁷¹ Generally, in the negligence context, the traditional risk-utility formula is used to determine whether the cost of a precaution is warranted, i.e., whether the cost is less than the probability of harm multiplied by the gravity of the resulting injuries. Firms should not have to take precautions to prevent reasonably unforeseeable security breaches.¹⁷² The problem of using the traditional risk-utility formula in calibrating negligence in Cyberspace lies in the lack of empirical data. One must first identify the costs of security breaches and then estimate their probability. There is little empirical data on the probability of harm, the severity of the harm and the burden of precaution for most Internet security breaches. Without valid data, it is difficult to determine the optimal way to allocate costs, and courts have little recourse in setting a reasonable standard of care for Internet security professionals.

168. *Id.* at 740.

169. Custom should be one factor, not the end result in the negligence formula. See RESTATEMENT (SECOND) OF TORTS § 295(A) (1965).

170. *Texas & Pacific R.R. Co. v. Behymer*, 189 U.S. 468, 470 (1903).

171. We are indebted to Guido Calabresi's insight that accidents are social problems that society should attempt to reduce in an optimum and efficient way. See generally GUIDO CALABRESI, *THE COST OF ACCIDENTS* (1961). A similar argument can be made about reducing preventable security breaches on the Internet, although these are arguably not accidents.

172. The Learned Hand risk-utility balancing test would excuse an Internet security provider from taking precautionary measures when the costs of such measures are greater than the potential loss. In such case, it is not negligent to fail to avoid the accident. If precautions are not cost-efficient, society is better off without precautions. See *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d. Cir. 1947).

Assuming that reliable data could be obtained, an optimal standard of care for Internet security would be one that increases societal welfare (and wealth) in the long run. It should not promote over- or under-investment in security precautions because both would be economically inefficient and could stunt the development of Internet security products, the growth of an Internet security profession and development of the NII.

It is possible that Internet security professionals will ultimately be subject to a higher professional standard of care such as that currently imposed upon doctors, lawyers and accountants. To date, however, courts have been slow to recognize the tort of "computer malpractice."¹⁷³ The New York Court of Appeals has stated the view taken by numerous courts:

A profession is not a business. It is distinguished by the requirements of extensive formal training and learning, admission to practice by a qualifying licensure, a code of ethics imposing standards qualitatively and extensively beyond those that prevail or are tolerated in the marketplace, a system for discipline of its members for violation of the code of ethics, a duty to subordinate financial reward to social responsibility, and, notably, an obligation on its members, even in non-professional matters, to conduct themselves as members of a learned, disciplined, and honorable occupation.¹⁷⁴

Unlike law or medicine, there is no licensing body or minimal education requirement for computer professionals.¹⁷⁵ When presented with a claim for "computer malpractice," courts have *en masse* declined to create a new tort for computer professionals.¹⁷⁶ While it seems clear that actions for professional negligence against computer-related "professionals" are foreclosed at this time, a nationalized training of Internet security professionals may arise as

173. Thomas G. Wolpert, *Product Liability and Software Implicated in Personal Injury*, 60 DEF. COUNS. J. 519, 521 (1993).

174. *Lincoln Rochester Trust Co. v. Freeman*, 311 N.E.2d 480, 483 (N.Y. 1974).

175. Wolpert, *supra* note 173, at 521.

176. See *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D. N.J. 1979) (rejecting new tort of "computer malpractice" for those who render computer sales and service), *aff'd*, 635 F.2d 1081 (3d Cir. 1980); *Hospital Computer Sys. v. Staten Island Hosp.*, 788 F. Supp. 1351, 1360-61 (D. N.J. 1992) (stating computer consultants do not meet the standard of "professionals" and thus can be held liable only for ordinary, not professional, negligence); *Analysts Int'l Corp. v. Recycled Paper Prods., Inc.*, No. 85-C8637, 1987 U.S. Dist. LEXIS 5611 at *16 (N.D. Ill. 1987) (stating Illinois does not recognize tort of computer malpractice for computer software systems designers, marketers and installers); *Invacare Corp. v. Sperry Corp.*, 612 F. Supp. 448, 453-54 (N.D. Ohio 1984) (refusing to recognize business negligence in computer-related setting as computer malpractice).

the NII matures, and therefore professional malpractice might follow.

Liability of Internet security providers may, nevertheless, be reviewed under the common law standard of negligence. As discussed, however, the indefinite nature of the common law standard of care offers little guidance to Internet security providers attempting to calculate their risk and plan their behavior. It gives perhaps even less guidance to courts faced with the challenge of reviewing those calculations in the aftermath of a security breach.

b. A Statutory Standard of Care

When a standard of care is set by a legislative enactment or regulation, courts will often find a defendant who violates it negligent per se.¹⁷⁷ In *Osborne v. McMasters*,¹⁷⁸ a court imposed negligence liability on a pharmacist for supplying plaintiff's decedent with unlabelled poison in violation of Minnesota's food and drug act. The *Osborne* court explained:

It is now well settled . . . that where a statute or municipal ordinance imposes upon any person a specific duty for the protection or benefit of others, if he neglects to perform that duty he is liable to those for whose protection or benefit it was imposed for any injuries of the character which the statute or ordinance was designed to prevent, and which were proximately produced by such neglect.¹⁷⁹

The *Restatement (Second) of Torts* follows this principle in validating statutory or administrative definitions of the proper standard of care.¹⁸⁰ In the interests of promoting the development of the National Information Infrastructure, the United States government could extend its internal standards for network and Internet security to the commercial sector. If the federal government were to develop commercial-sector standards for Internet security,¹⁸¹

177. In the negligence context, § 286 of the *Restatement (Second) of Torts* requires that a plaintiff prove that she is a member of the class of persons protected by the statute; that the statute protects against the particular interest invaded; and that she suffered the particular harm or hazard that was envisioned by the statute. See also *infra* note 190 and accompanying text.

178. 41 N.W. 543 (Minn. 1889).

179. *Id.*

180. RESTATEMENT (SECOND) OF TORTS § 286 (1965).

181. "Tort law is overwhelmingly common (state) law . . ." W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 3, at 19 (5th ed. 1984). Congress, however, has been increasingly receptive to proposals to federalize tort law. The GOP's Contract with America, which calls for common sense legal reform, inspired both the House and the Senate to pass comprehensive federal tort reform bills in 1995. The Senate passed the Product Liability Fairness Act of 1995 which will preempt state tort remedies for products liability. See S. 565, 104th Cong., 1st Sess.

then computer/software product manufacturers, computer/Internet security consultants and companies using networks and the Internet could all be found negligent per se for violating a statutory security standard.¹⁸²

The National Computer Security Center of the NSA administers the process for C2 certification of computer security.¹⁸³ Assuming that a federal certificate authority were widely adopted,¹⁸⁴ an Internet security firm that, for example, failed to obtain necessary "trusted certificate" authority for validating digital signatures might be found negligent per se for any loss resulting from such failure. Network-security device vendors might be required to market products under these or even higher standards. For example, they could be required to market "sniffless password" products or services which meet the standard of one-time passwords, i.e., passwords which cannot be reused because they are never transmitted across the Internet or via a modem in plain text.¹⁸⁵ The NSA adopted a "sniffless password" system in the 1980s on its Dockmaster Computer. Commercial enterprises could be required to emulate the NSA's example.

(1995). The Senate bill is aimed primarily at restricting punitive damages in products liability. In March of 1995, the House of Representatives passed the Common Sense Legal Standards Reform Act of 1995, which is a more comprehensive bill that restricts remedies in every substantive field of tort law. See H.R. 956, 104th Cong., 1st Sess. (1995). The nationalization of tort restrictions is presently stalled pending the reconciliation of differences between the Senate and House bills. See *House, Senate Set to Appoint Conferees on Product Liability Measure*, BNA WASHINGTON INSIDER, Oct. 30, 1995.

182. De facto evaluation of security products *vis-a-vis* government standards is already occurring. Novell, Inc. announced in August that they have formally applied for federal certification (Class C2) for their general purpose network operating system, "NetWare 4." According to IDG's Information Security service research director, "a C2 rating . . . has become a standard for commercial businesses as well as government and military organizations. Customers are using it as a differentiator when making product purchasing decisions." *NetWare 4 Enters Final Phase of C2 Evaluation; On Track to Receive First Client-Server Network Rating*, PR NEWSWIRE, Aug. 28, 1995 (statement of John Pescatore). Susan Biagi argues that commercial-sector security standards are derived from government-published standards. Biagi, *supra* note 52, at 37.

183. *The Trusted Network*, INFOWORLD, Aug. 22, 1994, at 51. C2 ("Controlled Access Protection") is the minimum rating federal agencies must comply with to protect sensitive but unclassified information. For further information on the details of the government's certification rating system, see *supra* note 55.

184. See generally Ellen Messmer, *Gov't Eyes Plans for a Public-Key Infrastructure*, NETWORK WORLD, July 11, 1994, at 8.

185. A "sniffless password" protocol utilizes a "random challenged calculated response method," which transmits a one-time cryptographically-generated password and provides solid identification and authentication. *Reports*, COMPUTER FRAUD & SECURITY BULLETIN, Aug. 1, 1994, 1994 WL 2299920, at *2.

Originators of commercial transactions on the Internet could be required to use an Internet-accessible digital notary system which "automatically detects if electronic documents have been tampered with or backdated."¹⁸⁶ The system can certify that database records, e-mail, word-processing or any other digital documents have not been tampered with by interlopers.¹⁸⁷ The Digital Notary has features such as the "digital fingerprint" and a validation feature.¹⁸⁸ The NSA has tested such a system for its electronic mail system and could require its use in commercial Internet enterprise.

Currently, there are no statutes requiring any of these higher Internet security standards, but this laissez-faire era may soon be over.¹⁸⁹ The creation of higher standards for the commercial sector would likely be a double-edged sword. While assurance of security is crucial to the development and capitalization of the NII, too much risk of liability could impede development.

In the event of the adoption of federal certification, an additional issue will need to be resolved. Some jurisdictions provide that the violation of a statutory rule is only some evidence of negligence in determining whether a defendant exercised due care in the circumstances.¹⁹⁰ Other jurisdictions provide that an unexcused violation of a statute is negligence per se as to consequences that the statute was designed to prevent.¹⁹¹ The probative value of statutory rule violation would need to be harmonized among the jurisdictions.

c. Application of Negligence Doctrine: On-line Service Providers

The rise of commercial on-line service providers such as CompuServe, Prodigy, America Online and Delphi raises novel security liability issues. The primary question is whether a company assumes a greater duty of care when it decides to implement Internet security, as Prodigy Services Co. (Prodigy) was deemed to have done when it screened messages on its "Money Talk" bulletin board.¹⁹²

186. *Internet-Accessible Digital Notary System Detects Electronic Record Tampering*, PR NEWSWIRE, Jan. 17, 1995.

187. *Id.*

188. *Id.*

189. Jared Sandberg, *On Line: Regulators Try to Tame the Untamable On Line World*, WALL ST. J., July 5, 1995, at B1.

190. WILLIAM L. PROSSER, *LAW OF TORTS* 201 (4th ed. 1971).

191. *Id.* at 200.

192. For excellent pre- and post-decision discussions of the *Prodigy* case, see Matthew Goldstein, *Prodigy Case May Solve Troubling Liability Puzzle*, NAT'L L.J., Dec. 19, 1994, at B1; John B. Kennedy et al., *Defamation Law*, NAT'L L.J., July 10, 1995, at B7.

Prodigy, a commercial on-line service provider (OSP), uses software which detects objectionable words and automatically notifies the user that their message will be censored.¹⁹³ After a message accusing Stratton Oakmont, Inc. of fraudulent securities offerings appeared on Prodigy's electronic bulletin board, Stratton Oakmont, filed a defamation lawsuit demanding \$100 million in punitive damages from Prodigy.¹⁹⁴ Prodigy defended on the grounds that it was primarily a passive conduit of information and not a publisher.¹⁹⁵ The district court held Prodigy to the higher standard of a publisher, even though Prodigy did not originate the defamation but only passed it on to its users.¹⁹⁶ The district court stated that, by reviewing and deleting notes from its bulletin boards on the basis of offensiveness, Prodigy "is clearly making decisions as to content... and such decisions constitute editorial control."¹⁹⁷ On October 24, 1995, the *Prodigy* case was settled while the appeal was pending. In an unusual procedural move, Stratton Oakmont agreed to drop its demand for \$100 million damages for defamation in an exchange for Prodigy's apology.¹⁹⁸ Stratton Oakmont also agreed not to contest Prodigy's motion to ask the court to reverse or set aside its previous ruling on Prodigy's status as a publisher.¹⁹⁹ The court's opinion, while unpublished and lacking precedential value,²⁰⁰ nevertheless provides a ready-made line of argument for the next time similar issues arise.

The circumstances of the *Prodigy* dispute raise important legal questions to be addressed in future litigation. If OSPs are to be held to a higher standard of care, and are thus potentially liable for defamation, might they also be liable for misappropriation, invasion of privacy, viruses, stalking, harassment or child pornography on

193. Rex S. Heinke & Heather D. Rafter, *Rough Justice in Cyberspace: Liability on the Electronic Frontier*, COMPUTER LAWYER, July 1994, at 1.

194. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (S.D.N.Y., May 26, 1995) (unpublished decision).

195. *Id.* The *Prodigy* case was critiqued in many electronic discussion groups on the Internet. Professor I. Trotter Hardy stated that sentiment is running "in favor of Prodigy and for unfettered expression on computer bulletin boards." Goldstein, *supra* note 189, at B1 (quoting Professor Hardy). Some courts have been reluctant to find bulletin board operators liable for the torts of their customers. See *Cubby Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (rejecting defamation claim against on-line service on the grounds that it was not a publisher since it exercised no editorial control over the content of statements posted on its bulletin boards).

196. *Prodigy*, 1995 WL 323710 at *10.

197. *Id.*

198. Peter H. Lewis, *After Apology From Prodigy, Firm Drops Suit*, N.Y. TIMES, Oct. 25, 1995, at D1.

199. *Prodigy, Plaintiff Reach Agreement in Libel Case, Deal May Let On-Line Firms Off the Hook*, CHI. TRIB., Oct. 25, 1995, at 3.

200. *Prodigy*, 1995 WL 323710 at *1.

their systems? If an OSP uses security products or technologies to guard against such acts, might the product/technology vendor, licensor, or installer be deemed potentially liable as well, as defendants in an unbroken chain of product distribution? Might liability be more likely to attach if such acts occur due to a security breach? To security laxity? Today, no one thinks twice about dropping sensitive documents, contracts and letters in the mail, though the possibility of theft or destruction, invasion of the correspondents' privacy, or transmittal of defamatory or obscene material exists. If any of these occur, the United States Post Office is not held liable.²⁰¹ Yet the *Prodigy* result may foreshadow a standard whereby an OSP would be held liable for such incidents even though it attempted to deter their occurrence.

The *Prodigy* opinion calibrated the standard of care too high. If that standard is followed, an on-line service that provides hosts to monitor children's chat-areas might find that it has assumed liability of unknown and unknowable magnitude. Despite the *Prodigy* decision's unpublished status, the court's ruling that Prodigy is a publisher casts a cloud of uncertainty over the information highway.

OSPs may be liable for other torts committed by their patrons. For instance, the Clinton Administration's Working Group on Intellectual Property and the National Information Infrastructure has recommended that OSPs be governed by tort law for copyright-infringing materials uploaded to their systems.²⁰² In their final report ("the White Paper"), the Working Group declared that vicarious liability for copyright infringement was appropriate because lowering the liability standard for OSPs would be "a significant departure from current copyright principles and law and would result in a substantial derogation of the rights of copyright

201. The Federal Torts Claims Act provides that claims against the U.S. Postal Service are barred by sovereign immunity. Federal Tort Claims Act, 28 U.S.C. § 2680(b) (1995); *U.S. v. Atlantic Coast Line Ry. Co.*, 215 F. 56 (4th Cir. 1914) (holding the government is not responsible to the owner of mail lost in transit). The U.S. government is deemed to be engaging in a governmental function when it delivers and transports mail. The government is liable to owners of lost or damaged mail only to the extent that it has consented to be liable. *Taylor v. U.S. Post Office Dept.*, 293 F. Supp. 422 (E.D. Mo. 1968); see also *Twentier v. United States*, 109 F. Supp. 406, 124 Ct. Cl. 244 (1953) (holding the United States is liable to the owners of lost and damaged mail only to the extent to which it has consented to be liable and to the extent that liability is defined by the postal laws and regulations).

202. U.S. PATENT AND TRADEMARK OFFICE INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP IN INTELLECTUAL PROPERTY RIGHTS 114 (Final Report, Sept. 5, 1995) (the White Paper).

owners."²⁰³ One reviewer of the White Paper ascribed the Working Group's decision to maintain a high standard for OSPs, in part, to "confidence that advances in encryption, digital cash, digital signatures and other *electronic security mechanisms* will allay the fears of distributors and content owners alike."²⁰⁴

If OSPs can be held liable for infringing material on their services, there is little reason why an Internet service providers (ISP) should not be liable for infringing material uploaded by its customers to Web sites resident on its server computers. ISPs, as well as OSPs, are likely to continue to develop and implement new security technologies in order to compete in the Internet access market. The White Paper indicates that ISPs' increased attention to security will directly impact their liability.

In addition, while OSPs are far from the functional equivalent of Internet security professionals, their activities are inextricably linked and may well become more so in the future as the technologies evolve. Not only may the reliance on Internet security technologies lead to stricter standards for OSPs and ISPs, but Internet security professionals and product makers might also face increasing copyright-related liability as they are asked to deliver increasingly effective on-line security products.

It is not surprising that vicarious tort liability, targeting service providers rather than private individuals, has been the epicenter of conflict over the appropriate role of tort law on the information highway. Individual on-line tortfeasors can avoid repercussions for their actions by simply disguising their messages and postings.²⁰⁵ While this frequently prevents plaintiffs from locating an Internet stalker or other intentional tortfeasor,²⁰⁶ some Internet security products now provide the user with some ability to track tortfeasors or block their access to protected systems.

Licensors of Internet security products could certainly be subject to independent torts arising out of a breach of contract. For example, a licensor of an Internet security product could be subject to the independent tort of fraud or misrepresentation if it marketed a device known to lack the qualities advertised. However, the overarching question is whether new tort doctrines are required to accommodate the new Internet security products. Should the tort law for security products be little more than new wine in old bottles?

203. *Id.*

204. John Kennedy & Mary Rasenberger, *Does Cyberspace Merit a New Legal Order?*, N.Y. L.J., Oct. 4, 1995, at 1 (emphasis added).

205. Branscomb, *supra* note 153, at 1643.

206. *Id.*

For the licensor of nationally-marketed security products, there is the additional problem of whose tort law applies. Tort law is traditionally state law and thus there are fifty different tort regimes. The problem is compounded by the internationalization of the sale of security products.²⁰⁷ Internet security products are not only sold within the continental United States, they are distributed to more than 100 countries via the Internet.

As this discussion demonstrates, common law tort doctrine is an inefficient means of allocating risk in the Internet security market. At this point in time, there is little case law or commentary applying negligence theory to computer software and service providers. As reliance on Internet security technologies increases, it becomes more important to protect and encourage security software and related service providers in the market. Reliance on nonexistent, inconsistent or vague standards of negligence liability could defeat this goal.

2. STRICT PRODUCTS LIABILITY

Products liability generally refers to legal liability of manufacturers for injuries caused by the marketing of products. Strict products liability grew out of a societal judgment "that people need more protection from dangerous products than is afforded by the law of warranty."²⁰⁸ Basically, strict products liability permits an injured consumer to recover damages for physical injury or property damages from a manufacturer upon a showing that the manufacturer distributed

207. Tort law presents intractable problems of conflicts of law. The first reported appellate opinion applying defamation in Cyberspace was the Australian case of *Rindos v. Hardwick*, No. 1994 of 1993 (W. Austl. Sup. Ct. Mar. 31, 1994) (discussed in Geoff Thomas, *\$40,000 Awarded in First Cyberspace Defamation Case*, AUSTRALIAN FINANCIAL REVIEW, May 4, 1994 (available on LEXIS, AUST Library, AUSNEWS file)). In *Rindos*, an Australian anthropologist allegedly defamed a fellow Australian anthropologist on the Internet, accusing him of engaging in pedophilia and of being professionally incompetent. The Supreme Court of Western Australia awarded the plaintiff \$40,000, the largest defamation award in the past four years.

The *Rindos* case highlights the frailties of applying tort law to redressing conflicts on the Internet. Suppose the defamatory communications had crossed international borders? Suppose the anthropologist had been defamed, not by a fellow Australian, but by a citizen of Saudi Arabia? Would the anthropologist really have a reputational interest in Saudi Arabia? If the anthropologist were a person of some fame, could the Saudi defendant rely upon the doctrine of limited public figure, which is an American rule? The problem of jurisdiction is another problem with tort law. What jurisdiction would apply? The jurisdiction of where the alleged defamation arose, or where it was received? Contract law, in contrast, permits the parties to chose a forum state so long as it bears a reasonable relationship to the contract or the parties.

208. *East River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 866 (1986).

a product²⁰⁹ containing a dangerous defect²¹⁰ into the stream of commerce, and that the defective product caused the injury.²¹¹ Neither negligence nor privity must be proved.²¹² The vast majority of American jurisdictions have adopted this standard over the past thirty years.²¹³

Strict products liability would pose great advantages for purchasers damaged by Internet or Internet security products. For example, strict products liability offers recourse to third parties who would be excluded from breach of contract actions due to lack of privity. Additionally, buyers avoid the notice requirement and are shielded from vendor-imposed liability limitations that are part and parcel of the U.C.C.²¹⁴

209. The Third Circuit has held that when computer programs are "implanted in a medium," they are "tangible, moveable" and become "products." *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670, 675-76 (3d Cir. 1991). If an Internet security measure were deemed not to be a "product," strict products liability could not apply. *See, e.g., Salomey v. Jeppesen & Co.*, 707 F.2d 671, 676-77 (2d Cir. 1983) (rejecting argument that producing navigation charts is a service and holding they are products for purposes of Restatement § 402A); *Aetna Casualty & Sur. Co. v. Jeppesen & Co.*, 642 F.2d 339, 342-343 (9th Cir. 1981) (holding navigation charts to be products).

210. RESTATEMENT (SECOND) OF TORTS § 402A (1964).

211. The plaintiff need only establish that a defect in software proximately caused injury or damage to recover in strict products liability. *See generally* Diane B. Lawrence, *Strict Liability, Computer Software and Medicine: Public Policy at the Crossroads*, 23 TORT & INS. L.J. 1 (1987). For a discussion of Internet security products see *infra* part II.B.

212. RESTATEMENT (SECOND) OF TORTS, § 402A (1964).

213. Most jurisdictions have adopted some version of § 402A of the *Restatement (Second) of Torts*, which states:

Special Liability of Seller of Product for Physical Harm to User or Consumer

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

(a) the seller is engaged in the business of selling such a product, and

(b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

(2) The rule stated in Subsection (1) applies although

(a) the seller has exercised all possible care in the preparation and sale of his product, and

(b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.

RESTATEMENT (SECOND) OF TORTS § 402A.

214. The U.C.C. will be discussed in detail in the *infra* part III.B. The U.C.C. requires buyers to give notice of defects to sellers. U.C.C. § 2-607(3)(a) (1990). Section 2-719 allows vendors to limit damages and remedies, but places constraints on the extent of limitation:

Thomas Wolpert posits possible scenarios where failed software²¹⁵ may be unreasonably dangerous or "place life and limb in peril."²¹⁶ The hypothetical situations involve:

An energy management system in a high school that was programmed to be inoperable until 6:30 a.m. and that prevented an exhaust fan in a chemistry lab from working, thus causing a teacher to inhale chlorine gas.

A computer system that generated a warning label for a prescription drug that was inadequate and that the pharmacist failed to use anyway.

A computer system used by a pretrial service agency that failed to warn an arraignment judge that an arrestee was out on bond for two previous armed robberies, a circumstance that resulted in the release of the arrestee and grave injuries to a person wounded in another armed robbery attempt.

A defective computer and software program that were used to assist in calculating doses of radiation received for patients who were being seeded with radioactive implants to treat cancer of the prostate.²¹⁷

The policy interest in preventing "the marketing of products having defects that are a menace to the public" is strong.²¹⁸ The manufacturer, even if not negligent in the manufacture of the product, is best situated to prevent such products from reaching the market, and bears the risk of such occurrences.²¹⁹ Given this policy, the above cases would seem appropriate for strict products liability treatment. Some commentators favor extending strict liability to defective software where personal injury is the result.²²⁰

(2) Where circumstances cause an exclusive or limited remedy to fail of its essential purpose, remedy may be had as provided in this Act.

(3) Consequential damages may be limited or excluded unless the limitation or exclusion is unconscionable. Limitation of consequential damages for injury to the person in the case of consumer goods is prima facie unconscionable but limitation of damages where the loss is commercial is not.

U.C.C. § 2-719 (1990).

215. Wolpert, *supra* note 173, at 519.

216. Products liability grew out of this famous statement made by Judge Cardozo in *MacPherson v. Buick Motor Co.*, 111 N.E. 1051, 1053 (N.Y. 1916).

217. Wolpert, *supra* note 173, at 519.

218. *Escola v. Coca Cola Bottling Co. of Fresno*, 150 P.2d 436, 441 (Cal. 1944) (concurring opinion).

219. *Id.*

220. See, e.g., Brannigan & Dayhoff, *supra* note 162, at 130; Susan Lanove, *Computer Software and Strict Products Liability*, 20 SAN DIEGO L. REV. 439, 456 (1983); Patrick T.

While courts have decided that products liability can apply to manufacturers of defective computer programs,²²¹ they have been reluctant to actually extend strict products liability to computer software.²²² Wolpert observes that strict products liability actions have "been slow to develop against the vendors of software."²²³ Given this reluctance, it seems unlikely that courts would apply strict products liability to defective Internet security products which injure only property.²²⁴

Where the only damage is to the Internet security product, courts would likely apply warranty law, rather than strict products liability. In *East River Steamship Corp. v. Transamerica Delaval, Inc.*,²²⁵ the United States Supreme Court refused to apply strict products liability in admiralty in a case where the only loss was to the product itself. The Court reasoned that contract and warranty law were better suited to deal with commercial losses than was strict products liability. The Court stated that if products liability were extended too far, "contract law would drown in a sea of tort."²²⁶

3. DEFENSES

The history of tort law has been characterized by the creation of defenses and immunities from legal liabilities.²²⁷ In the nineteenth

Miyaki, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121 (1992).

221. See, e.g., *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D. N.J. 1979), *aff'd*, 635 F.2d 1081 (3d Cir. 1980).

222. See *id.*

223. Wolpert, *supra* note 173, at 519. Most commentators contend that strict liability should not apply to defective software, since computer software is predominately a service. See, e.g., Roy N. Freed, *Products Liability in the Computer Age*, 17 JURIMETRICS J. 270 (1977).

224. In the course of strict products liability evolution, a manufacturer's duty of care was broadened to include protection against property damage. See *Marsh Wood Prods. Co. v. Babcock & Wilcox Co.*, 240 N.W. 392, 399 (Wis. 1932); *Genesee County Patrons Fire Relief Assn. v. L. Sonneborn Sons, Inc.*, 189 N.E. 551, 553-55 (N.Y. 1934). A majority of courts have held that such damage has to be to property other than the defective product itself. See *Seely v. White Motor Co.*, 403 P.2d 145 (Cal. 1965); *Jones & Laughlin Steel Corp. v. Johns-Manville Sales Corp.*, 626 F.2d 280, 287 & n.13 (3rd Cir. 1980). A minority of courts have held that strict liability may encompass cases where the only property damage is to the defective product itself. See *Emerson G.M. Diesel, Inc. v. Alaskan Enterprise*, 732 F.2d 1468, 1474 (9th Cir. 1984) (declining to follow *Seely*); *Santor v. A. & M. Karagheusian Inc.*, 207 A.2d 305, 312-13 (N.J. 1965) (finding manufacturer liable where only loss was to defective carpeting).

225. 476 U.S. 858 (1986).

226. *Id.* at 866.

227. See MORTON J. HORWITZ, *THE TRANSFORMATION OF AMERICAN LAW 1780-1860*, 99-161 (1977).

century, courts carved out doctrines such as the fellow-servant rule, assumption of risk and contributory negligence to mitigate or absolve a defendant's wrongdoing. Morton Horwitz argues that the origin of these defenses served as a subsidization of economic growth for the developing industrialization.²²⁸ Such defenses would undoubtedly be raised in the realm of Internet security breach as well.

Perhaps, just as there may have been legal subsidies for economic development in the nineteenth century, courts could encourage the development of the NII by employing these legal doctrines to guarantee certainty and predictability of economic consequences today.²²⁹ During the early years of the NII, there may be a need to afford legal subsidies to those who capitalize the Internet. On the other hand, such subsidies could leave victims of devastating security breaches with no redress. For example, if a firewall were even inadvertently misused, the vendor of the firewall could assert product misuse and potentially escape liability. Or, if a company's network was illicitly entered from the Internet by a novel means after an Internet security consultant had been hired to recommend and assist in the implementation of hacker-proof security policies and products, the company's remedy could evaporate if the consultant could show the method of invasion was reasonably unforeseeable.

Moreover, courts would need to determine if damages would be affected when a victim of an Internet security breach fails to take "reasonable precautions." For example, most computer industry experts agree that the only secure passwords are ones that are a *minimum* of seven randomly-chosen letters, numbers and symbols.²³⁰ The shorter the password, the easier it is to crack. Thus, passwords that are too short or do not meet other criteria may invite the defense of contributory negligence.

As early as 1993, one Internet security expert declared that any password chosen in accordance with any of the following methodologies is insecure:

1. Modifying any part of your name or name plus initials;
2. Modifying a dictionary word;
3. Acronyms;
4. Any systematic, well-adhered-to algorithm. For instance,

228. *Id.*

229. *Id.* at 111.

230. *See, e.g.*, A LEC MUFFET, ALMOST EVERYTHING YOU EVER WANTED TO KNOW ABOUT SECURITY* (*BUT WERE AFRAID TO ASK!), Security.FAQ, version 2.2, Dec. 3, 1993, available at "ftp://coast.cs.purdue.edu/pub/doc/faq/faq-security.txt.z" on the World Wide Web.

never use passwords like: alec7 (it's based on the user's name (and it's too short anyway); tteffum (based on the user's name again); gillian (girlfriend's name—in a dictionary); naillig (ditto—backwards); PORSCHE911 (it's in a dictionary); 12345678 (it's in a dictionary and people can watch you type it easily); qwertyui (ditto); abcxyz (ditto); Oooooooooo (ditto); Computer (just because it's capitalized doesn't make it safe); wombat6 (ditto for appending some random character); 6wombat (ditto for appending some random character); nerde3 (even for French words); mr. spock (it's in a sci-fi dictionary); zeolite (it's in a geological dictionary) ze0lite (corrupted version of a word in a geological dictionary); ze01lte (ditto); Z30L1T3 (ditto).²³¹

The security expert concluded: "[T]hese examples emphasize that ANY password derived from ANY dictionary word (or personal information), modified in ANY way, constitutes a potentially guessable password."²³² With the increasing awareness of the importance of password security, judges may have little difficulty finding companies contributorily negligent if they do not bother to implement and adhere to acceptable password security recommendations. Soon, it may be contributorily negligent for a firm to permit any remote access to a router/gateway which is not protected by one-time passwords.

To further underscore the unwieldy nature of liability allocation by negligence law, consider the following scenario. Suppose a minor bypasses Internet security controls and is stalked by a pedophile on the Internet. Would the minor be found contributorily or comparatively negligent on the grounds that when a legal infant performs an adult activity, he is held to an adult standard of care? Would a minor's contributory negligence be imputed to the parent? Is surfing the Internet the functional equivalent of performing an adult activity, such as operating an automobile, airplane, snowmobile or powerboat? More generally, would the failure of a user to look out for his own security bar him from recovery for damages or expose him to suit by others?

Answers to questions such as these and the related issues discussed above will take years to be worked out in the courts. Using traditional tort doctrine to allocate liability for failed Internet security products raises as many questions as it answers. While tort law will have its place in Cyberspace, it is apparent that it fails as a primary framework for "regulating" Internet security products. Tort law cannot readily provide resolutions to the issues above. This

231. *Id.*

232. *Id.*

leaves manufacturers, vendors, consultants and users of Internet security products unsure where they stand with respect to liability. A more certain framework is desirable so that the growth of the NII will not be impeded by uncertainty in the law. Given the drawbacks of a tort law paradigm, we turn to an examination of contract principles and their potential efficacy in affording a workable framework for allocation of liability with respect to failed Internet security products.

B. Regulation Under Current Contract Law

Contract law is the principal mechanism for facilitating market transactions.²³³ Since contract law permits "individuals to pursue their voluntary choices,"²³⁴ several commentators argue that contract law provides the legal ground rules of the Internet.²³⁵ This part examines the appropriateness of contract law as a general framework for allocating the risks and liabilities that arise out of commercial transactions involving Internet security products. First, we survey the effectiveness of applying traditional contract theory. Then we examine the application of U.C.C. Article 2 sales principles to Internet security product transactions.

1. TRADITIONAL NOTIONS OF CONTRACT LAW

Modern contract law has its roots in the nineteenth century philosophy of the freedom of contract. Under this view, parties had broad freedom to make their own voluntary arrangements, and the courts' role was to interpret and enforce the parties' obligations by employing the principles of liberty, equality and reciprocity, the dominant values of a market economy.²³⁶ Contract law provided the means to permit parties to strike the deal they truly wanted, within the parameters of good faith and fair dealing, rather than a deal prescribed by some centralized authority.²³⁷ Yet, total freedom of contract allowed one contracting party to oppress the other whenever asymmetrical relationships of power and economic position between

233. See JOHN TILLOTSON, *CONTRACT LAW IN PERSPECTIVE* 3 (1981).

234. HUGH COLLINS, *THE LAW OF CONTRACTS* 1 (1986).

235. See generally Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 *JURIMETRICS J.* 1 (1994); Hardy, *supra* note 29; David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 *VILL. L. REV.* 487 (1993).

236. COLLINS, *supra* note 234, at 9.

237. JOHN COLLINGE, *TUTORIALS IN CONTRACT* 10-14 (1981).

the two parties existed.²³⁸ While classical contract theory ignored the law's role in legitimizing the position of the well-off who enjoy great power in the market,²³⁹ there has been a counter-movement in modern contract theory moderating the harsh consequences that stem from unequal bargaining power.²⁴⁰ Frederick Kessler's classic law review article addressed the problem of how courts should treat contracts where the lesser party is required to adhere to the terms of the stronger.²⁴¹ The lesser party is protected to a certain extent from being forced to comply with unfair terms of a contract by the application of the doctrine of unconscionability.²⁴² To this end, modern courts have increasingly scrutinized the underlying fairness of the contract where the parties are in vastly different bargaining positions.²⁴³

Modern contract law retains the flexibility and malleability of traditional contract theory. Since contract law enables the parties to forge unique solutions to emergent legal problems, it is particularly well suited for the new information technologies.²⁴⁴ Contract law's capacity to evolve as a voluntary social institution is in contrast with the coercive features of tort law. General contract law principles fit well with the emergent culture of the Internet, which eschews involuntary obligations, whether imposed from the state or from tort law. Commentators suggest that contract law, unlike tort (and criminal) law, is ideally situated to informally regulate unauthorized Internet access and hacker malfeasance.²⁴⁵ For instance, Robert Dunne believes that contract law conforms to the original Cyberians'

238. *Id.* at 11.

239. Professor Stewart Macaulay and his University of Wisconsin colleagues critique the law and economics idealization of contract theory as turning a blind eye to the ways that contract law legitimates and validates the position of the powerful and wealthy in society. STEWART MACAULAY, *CONTRACTS: LAW IN ACTION* 10 (1995). They note that the law and economics approach to contract theory fails to "deal with the justice or fairness of the present distribution of wealth, status, privilege or power in the society." *Id.*

240. See generally COLLINS, *supra* note 234.

241. Frederick Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

242. Arthur Leff subdivided the doctrine of unconscionability into procedural unconscionability (unfairness in striking a bargain) and substantive unconscionability (unfairness in the terms of the bargain itself). Arthur A. Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485 (1967).

243. COLLINS, *supra* note 234, at 67.

244. The abolition of the institution of imprisonment for breach of contract and the rise of compensatory principles in contract law were two key developments in modern contract law. See A.W.B. SIMPSON, *A HISTORY OF THE COMMON LAW OF CONTRACT* 601-02 (1975).

245. See Dunne, *supra* note 235, at 1.

aversion to centralized management and respects their desire for mutually-agreed-upon norms.²⁴⁶ Trotter Hardy also argues that the self-regulation aspect of contract law offers legal solutions for many legal issues arising in Cyberspace.²⁴⁷ He concludes:

[T]he rapidly changing technology of computer communications implies a need for flexible legal regulation of behavior, and that flexible regulation in turn implies a presumption that the most decentralized rules should be applied whenever possible. This will often entail contractual agreements worked out among the affected parties, rather than a broadly-applicable judicial or legislative resolution.²⁴⁸

The new information technologies are already employing contract law in the transnational space of the electronic frontier.²⁴⁹ David Johnson and Kevin Marks advocate "primary reliance on contracts to govern the Cyberspace environment."²⁵⁰ With respect to on-line service providers and consumers, these commentators maintain that contract law effectively governs key aspects of their relationships,²⁵¹ and that the "marketplace provides adequate incentives for all concerned to agree on the rules, once the general need for choice in the face of a flexible electronic environment is understood."²⁵²

Contract law, however, has limitations. For instance, contract law does not effectively address liability for injuries to third parties. While a licensor and licensee are free to contract, they are not free to discharge their legal obligations to unknown third parties injured by the failure of Internet security products. Accordingly, there will be a residual role for tort law when a third party is injured as the result of the failure of a security product. These third-party injuries may be economic or non-economic. For example, the Veterans Health Administration has a computer network including "172 medical centers, 350 outpatient clinics and 130 nursing homes nationwide."²⁵³ A doctor or other health practitioner in such a networked medical environment may be liable for permitting disclosures of confidential

246. See *id.* at 10-11.

247. See Hardy, *supra* note 29, at 995.

248. *Id.* at 995-96.

249. See Saskia Sassen, *Interdisciplinary Approaches to International Economic Law: When the State Encounters a New Space Economy: The Case of Information Industries*, 10 AM. U. J. INT'L L. & POL'Y 769, 772 (1995).

250. Johnson & Marks, *supra* note 235, at 489-90.

251. See *id.* at 490.

252. *Id.* at 514.

253. Silver, *supra* note 53, at 71.

patient information.²⁵⁴ Also, a bank may be liable for a security breach that results in confidential financial information being disclosed to a competitor or intruder.²⁵⁵

In addition to dealing with third-party issues, contract law in the digital age requires a specialized paradigm for dealing with the unique issues of contract formation, interpretation, performance, warranties and remedies. In particular, specialized ground rules for dealing with the transfer of rights in information technologies are needed. We next turn to the U.C.C. as a possible paradigm for resolving these issues.

2. CURRENT UNIFORM COMMERCIAL CODE

In this part, we argue that the U.C.C.'s Article 2 sales doctrine should not be applied to Internet security product transactions because it is fundamentally inconsistent with the commercial reality of such transactions.²⁵⁶ The goal of the U.C.C. is to forge and employ default rules that reflect commercial reality and balance the interests of diverse stakeholders in commercial transactions.²⁵⁷

a. Overview

The U.C.C. as a whole is "a single subject of law" that deals "with all of the phases which ordinarily arise in the handling of a

254. The release of confidential patient records violates the fiduciary relationship between physician and patient. Many states have statutes limiting the disclosure of a patient's health care information. See, e.g., California Confidentiality of Medical Information Act, CAL. CIV. CODE § 56 (1981) (defining circumstances under which health information may be disseminated to third parties); MONT. CODE ANN. § 50-16-501 (1987) (providing rules for disclosures of patient's health care information). Wrongful disclosure of patient records may also be the basis of tort actions based upon invasion of privacy, breach of fiduciary duty and the intentional infliction of emotional distress. See, e.g., *Banks v. Charter Hosp. of Long Beach*, 1992 WL 521069 (LRP Jury) (punitive damages awarded under an invasion of privacy action to a plaintiff who suffered emotional distress when her name and photograph appeared in an article about the defendant hospital without her consent); *Austin v. Methodist Hospital*, 1987 WL 231638 (LRP Jury) (awarding compensatory and punitive damages for unauthorized release of plaintiff's medical records of the strictest confidential nature). See also Annotation, *State Statutes or Regulations Expressly Governing Disclosure of Fact That Person Has Tested Positive for Human Immunodeficiency Virus (HIV) or Acquired Immunodeficiency Syndrome (AIDS)*, 12 A.L.R. 5th 149 (1994).

255. See generally Edward L. Raymond, Jr., Annotation, *Bank's Liability Under State Law, for Disclosing Financial Information Concerning Depositor or Customer*, 81 A.L.R. 4th 377 (1994).

256. Contract law generally requires a legal infrastructure advancing commercial practices. See Charles J. Goetz & Robert E. Scott, *The Limits of Expanded Choice: An Analysis of the Interaction Between Express and Implied Contract Terms*, 73 CAL. L. REV. 261 (1985).

257. U.C.C. §§ 1-102(1), (2) (1990).

commercial transaction."²⁵⁸ The goals of the U.C.C. were "to simplify, clarify and modernize the law governing commercial transactions."²⁵⁹ The U.C.C. was also intended "to permit the continued expansion of commercial practices through custom, usage and agreement of the parties."²⁶⁰

The U.C.C.'s overarching comprehensiveness can be illustrated by analyzing a commercial transaction. Imagine a sale of turkeys by a Minnesota farmer to the Big Super Market chain in Massachusetts. If the farmer is defined as a merchant, his turkeys must meet certain minimum quality standards, even if he makes no representations regarding the quality of his turkeys. If the turkeys never arrive at Big Super's loading dock, Big Super may have seller's remedies under Article 2. In the event of Big Super's default, the farmer might obtain an Article 9 security interest in the turkeys. The check issued by Big Super's manager in payment would be covered by Article 3 of the U.C.C. governing negotiable instruments. If the farmer deposits the check into his bank account, Article 4, which deals with the collection of checks and the relationship between the bank and the customer, is triggered. If the goods are stored or shipped, they may be covered by a bill of lading or warehouse receipt under Article 7. The U.C.C. deals with all of the stages in the life of a commercial transaction—from cradle to grave.

U.C.C. Article 2 is consistent with freedom of contract because it permits buyers and sellers to vary most provisions by agreement.²⁶¹ However, the parties are not free to disclaim "the obligations of good faith, diligence, reasonableness and care" ²⁶² The U.C.C. serves as a default model, supplying "gap-filler" contract terms for those the parties do not negotiate.²⁶³ Using the U.C.C. is analogous to buying a suit "off the rack." The alternative is to have a suit tailored to your specific body dimensions. Article 2 is composed of default or "off the rack" contract terms. If the parties are dissatisfied with Article 2's

258. U.C.C. pmb. (1990).

259. U.C.C. § 1-102(2)(a) (1990).

260. U.C.C. § 1-102(2)(b) (1990).

261. See U.C.C. § 1-102 Official Comt. 2 (1990) (stating that "freedom of contract is a principle of the [U.C.C.]"). The U.C.C.'s freedom of contract is tempered by the concepts of good faith and commercial reasonableness that permeate the statute. Section 1-203, for example, provides that "[e]very contract or duty within [the U.C.C.] imposes an obligation of good faith in its performance or enforcement." See generally Dennis M. Patterson, *Wittgenstein and the Code: A Theory of Good Faith Performance and Enforcement Under Article Nine*, 137 U. PA. L. REV. 335 (1988).

262. U.C.C. § 1-102(3) (1990).

263. See U.C.C. §§ 2-304 to -310 (1990).

default terms, they are always free to tailor their own sales contract solution.

b. Application of U.C.C. Article 2 to Internet Security Products and Services

Robert Feldman notes that "the information age is working profound changes in every area of the law."²⁶⁴ Sales law and licensing law have not escaped this influence.²⁶⁵ This part examines how the emerging information technologies pose new challenges for traditional sales law.

A contract for the sale of goods is one in which a seller agrees to transfer goods that conform to the contract in exchange for valuable consideration.²⁶⁶ Article 2 of the U.C.C. applies to "transactions in goods."²⁶⁷ There are some questions whether Internet security products are 'goods' within the scope of Article 2. Internet security products typically consist of or incorporate software. "Software" is defined in a proposed revision of the U.C.C. as "a computer program in source code, object code or in any other form, together with any associated data, program description, media and supporting documentation."²⁶⁸ Software may have a tangible aspect to the extent that it resides in various forms of media, but it also has intangible attributes which allow it to change form and appearance like a chameleon. Software is typically licensed, not sold; like Internet security products, it is transferred by a combination of sales/licensing transaction.²⁶⁹ Software is also intellectual property, subject to the regime of federal statutory law.²⁷⁰

Software is already treated as within the scope of U.C.C. Article 2 by the vast majority of courts. Some courts struggle with the intangible qualities of software, applying the U.C.C. by analogy.²⁷¹ Generally, courts distinguish between "sales" and "services": The former is governed by Article 2 whereas the latter falls under the

264. Robert A. Feldman, *A New Draft of UCC Article 2: A High Tech Code Takes Form*, 12 *COMPUTER LAW* 1 (Feb. 1995) [hereinafter Feldman, *New Draft*].

265. *Id.*

266. U.C.C. § 2-301 (1990).

267. U.C.C. § 2-102 (1990).

268. U.C.C. § 2-104(43) (Proposed Draft, Feb. 10, 1995).

269. This commercial reality is reflected in the Internet security product "sales and license agreement" reproduced in Appendix A, *infra*.

270. See generally 17 U.S.C. §§ 101-1101 (1994) (copyright); 35 U.S.C. §§ 1-376 (1988 & Supp. 1993) (patent).

271. Herbert J. Hammond, *Limiting and Dealing With Liability in Software Contracts*, 9 *COMPUTER LAW* 22 (June 1992).

auspices of the common law.²⁷² Courts look to the "predominant purpose" of a software agreement to determine which law should be applied.²⁷³ In light of this distinction, a difficult question concerns vendors who install software security products *and* have continuing service obligations.²⁷⁴

If Article 2 applies, a vendor of security products who claims his products to be "hacker-proof," "bullet-proof" or "air tight" could be subject to the express warranty obligations of the U.C.C.²⁷⁵ A vendor, however, could argue that these statements are mere sales talk or "puffing" and not definite enough to constitute warranties.²⁷⁶ Despite the damage to the buyer's intellectual property,²⁷⁷ courts customarily apply the U.C.C. rather than strict products liability to faulty software claims.

272. The bifurcated treatment of sales and services was first conceived centuries ago in the law-merchant tradition. See *Milau Assocs., Inc. v. North Ave. Dev. Corp.*, 368 N.E.2d 1247 (N.Y. 1977).

273. With hybrid transactions involving both sales and service, only transactions which are predominately sale of goods are within Article 2. If a court determines that services predominate, common law principles apply. See *Micro-Managers, Inc. v. Gregory*, 434 N.W.2d 97, 100 (Wis. Ct. App. 1988) (holding that under the predominant factor test, contract to develop software was not subject to U.C.C. because it was for services not goods); *Bonebrake v. Cox*, 499 F.2d 951, 960 (8th Cir. 1974) (holding that for a mixed contract, test is whether predominant factor, thrust and purpose is rendition of services).

Some courts are now applying William Hawkland's "gravamen" test. E.g., *Anthony Pools v. Sheehan*, 455 A.2d 434 (Md. 1983) (applying gravamen test to mixed sales and service transaction involving inground swimming pool with diving board). Dean Hawkland defines the gravamen test as follows:

Unless uniformity would be impaired thereby, it might be more sensible and facilitate administration, at least in this grey area to abandon the "predominant factor" test and focus instead on whether the gravamen of this action involves goods or services. For example, in *Worrell v. Barnes*, if the gas escaped because of a defective fitting or connector, the case might be characterized as one involving the sale of goods. On the other hand, if the gas escaped because of poor work by Barnes the case might be characterized as one involving services, outside the scope of the U.C.C.

I.W. HAWKLAND, UNIFORM COMMERCIAL CODE SERIES § 2-102:04 at Art.2, at 12 (1982); see also PETER B. MAGGS ET AL., *COMPUTER LAW: CASES, COMMENTS, QUESTIONS* 386 (1991).

274. There is little case law or commentary on applying warranties to services. See Robert A. Feldman, *Warranties and Computer Services: Past, Present and Future*, 10 *COMPUTER LAW* 1 (Feb. 1993) [hereinafter Feldman, *Warranties*].

275. U.C.C. § 2-313 (1990).

276. Express warranties are provided for under U.C.C. § 2-313, the implied warranty of merchantability under U.C.C. § 2-314, and the implied warranty of fitness for a particular purpose under U.C.C. § 2-315.

277. See generally Wolpert, *supra* note 173.

In addition, under the Article 2 sales regime, Internet security vendors could be subject to implied warranties of quality. To establish a breach of an implied warranty of merchantability, for example, the plaintiff would need only prove that an Internet security product was not merchantable²⁷⁸ at the time of sale (or licensing) and that injury or damage was caused proximately, and in fact, by the security product.²⁷⁹ Therefore, the failure of an Internet security product to prevent a hacker from entering a computer could potentially be actionable under an implied warranty if it could be proved that the security device was below the standard of other security products on the market.

On the other hand, the U.C.C. allows vendors to disclaim implied warranties, limit their liability and restrict buyers' remedies within the parameters of good faith, commercial reasonableness and conscionability. The extent to which vendors could use such disclaimers and limitations of liability to reallocate contract liability in Internet security contracts is unclear. Section 2-719 permits parties to set their own remedies and measure of damages.²⁸⁰ Internet security vendors often provide an "exclusive remedy" in lieu of remedies normally available under the U.C.C.²⁸¹ The vendor of a pre-packaged firewall product might attempt to limit liability to the "exclusive," but limited remedy of repairing or replacing the equipment and software.²⁸² Where the court finds the provision to be unconscionable, however, a network security vendor is neither free to agree upon an "exclusive" but nugatory remedy nor permitted to limit or exclude consequential damages.²⁸³ The court will not enforce a remedy that "fail[s] of its essential purpose."²⁸⁴ Thus, the sole remedy of repairing or replacing the Internet security software might not be enforced. If a court refuses to enforce such provisions, the aggrieved buyer will have the full panoply of Article 2 remedies at

278. "Merchantable goods" are those which "at least (a) pass without objection in the trade under the contract description . . . and (c) are fit for the ordinary purposes for which such goods are used . . . and (f) conform to the promise or affirmation of fact made on the container or label if any." U.C.C. § 2-314(2) (1990).

279. U.C.C. §§ 2-714, 715 (1990).

280. U.C.C. § 2-719 (1990).

281. U.C.C. § 2-719(1)(b) (1990).

282. See generally DeLois T. Leapheart, *Contractually Limiting Liability*, 72 MICH. BUS. L. J. 546 (1993); Note, *U.C.C. Section 2-719: Limited Remedies and Consequential Damage Exclusion*, 74 CORNELL L. REV. 359 (1989); Roy Ryden Anderson, *Contractual Limitations of Remedies*, 67 NEB. L. REV. 548 (1988). See also *infra* App. A §14(b).

283. U.C.C. § 2-719(3) (1990).

284. U.C.C. § 2-719(2) (1990).

her disposal.²⁸⁵ If the disclaimers are enforced, the licensee would be allocated the costs of the security breach. A licensee would then bear the costs of all tort and statutory actions based upon unexcused disclosures of confidential information.

Article 2 not only fails to provide answers to the complex contracting questions posed by software transactions, but also fails to resolve the basic question: Is the licensing of software the sale of a "good" covered by U.C.C.²⁸⁶ or a "service"? The U.C.C. has not enabled the modernization of commercial law pertaining to software, Internet security products and other intangibles. At present, vendors of Internet security products lack an accessible and determinate body of law.²⁸⁷

3. ARTICLE 2 SALES VERSUS LICENSING OF INTANGIBLES

Judges and practitioners find Article 2 inadequate when it comes to the new information technologies.²⁸⁸ It is doctrinally inconsistent for Article 2 to cover both the "sale of tangibles" and the "licensing of intangibles." Article 2 of the U.C.C. deals with the *sale of tangible goods*; network security products typically involve the *licensing of intangibles*.

A "sale" is defined by the "passing of title from a seller to a buyer for a price."²⁸⁹ In transactions governed by Article 2, title passes from buyer to seller.²⁹⁰ In contrast, title typically does not pass in the licensing of an Internet security product. Rather, licensing is a lower-order transfer of property interest conveying a right to use electronic information and other intangibles for a designated period of time or under designated conditions. The licensing of intangibles, like

285. U.C.C. § 2-719 (1990).

286. Bonna Lynn Horovitz, Note, *Computer Software As a Good Under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth*, 65 B.U. L. REV. 129 (1985).

287. Karl N. Llewellyn, *Why We Need the Uniform Commercial Code*, 10 U. FLA. L. REV. 367, 369 (1957) (explaining the purpose of the U.C.C. as a codification project to promote accessibility and efficient commercial transactions).

288. See generally Jonathan Groner, *This Uniform Code Does Not Compute: Software Industry Balks at Rewrite of Commercial Law*, LEGAL TIMES, Nov. 1, 1993, at 1 (contending that the ground has moved under the present version of Article 2 for all software licensing transactions).

289. U.C.C. § 2-106(1) (1990).

290. Section 2-401(1) provides that "title to goods passes from the seller to the buyer in any manner and on any conditions explicitly agreed on by the parties." U.C.C. § 2-401(1) (1990).

leases, validates the right to use all forms of intellectual property.²⁹¹ While the essence of a sale is the passing of title for a price,²⁹² with intangibles, the passing of title is only a vehicle for conveying valued intellectual property and the right to use that information.²⁹³ The title to tangible copies of intangibles is not dispositive or even relevant to any software licensing rights.²⁹⁴ The medium is not the message,²⁹⁵ only the right to exploit information.

An intangible may consist of data, information, software or intellectual property rights. Under Article 2, a buyer may freely assign her rights in the goods. In contrast, the typical security software license prohibits assignment and may have other use restrictions. Diagram One illustrates in tabular form the differences between a typical sales transaction and the licensing of security software.

291. Consumer finance leases are regulated by Article 2A of the U.C.C. Leases grant the limited right to use goods, whereas licenses are a limited right to use intangibles.

292. U.C.C. § 2-106(1) (1990).

293. See generally Steven O. Weise, *Article 9—Personal Property Secured Transactions*, 46 BUS. LAW. 1711 (Aug. 1991).

294. Robert Mitchell argues that the proposed U.C.C. § 2-2501(a) might state that "title to goods or tangible copies is not dispositive or relevant to any issue addressed in this chapter." See Memorandum from Robert B. Mitchell, Task Group Co-Leader to Donald A. Cohn & Ellen Kirsh, Co-Chairs, ABA Software Subcommittee, Business Law Section, American Bar Association, Parts 21 & 23 (Mar. 3, 1995) (on file with the *High Technology Law Journal*).

295. Marshall McLuhan's famous aphorism about television was that the "medium is the message." MARSHALL MCLUHAN, *UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN* 7 (1964). The medium in a licensing transaction is the diskette or other tangible vehicle. The proposed licensing chapter applies to the tangible copies of the intangible property leaving the rules for transferring intangibles to federal intellectual property law. See U.C.C. § 2-2501(a) (Proposed Draft, Feb. 10, 1995).

DIAGRAM ONE: LICENSING VERSUS SALES

Attribute	Licensing	Sale
Transfer of Title	Mass-marketed security products are typically licensed. No title passes. Customized Internet security transactions often involve the sale of hardware, the licensing of software and the procurement of services.	Title to goods passes when the buyer accepts and pays in accordance with the contract. U.C.C. § 2-301.
Use Restrictions	Location and use restrictions are typically specified in the license agreement.	Once title passes, typically no location or use restrictions exist in the sale of goods.
Norm of Confidentiality	Licensee is typically not permitted to resell or transfer materials after a rightful rejection. Licenses do not grant licensee a right to underlying data.	The sale of goods presumes no norm of confidentiality.
Delivery of Product	Intangibles may be "delivered" computer-to-computer without human contact.	The sale of goods is marked by a physical delivery of tangible goods. The buyer has the right to inspect goods. U.C.C. § 2-512.
Standard of Performance	Software is rarely, if ever, "bug-free." With the licensing of intangibles, substantial performance is the de facto performance standard.	Buyers of goods have a right to reject goods if they "fail in any respect to conform to the contract." U.C.C. § 2-601.
Remedies	Remedies may include remedies for breach of confidentiality or breach of the warranties against failure of system integration, or unauthorized access by third parties, viruses and extraneous data.	Sections 2-703 and 2-711 of Article 2 index the range of remedies with respect to the sale of goods.
Nature of Relationship	Mass-marketed licenses are one-shot transactions. Customized license agreements are generally relational and long-term. Vendors often customize, support or maintain software.	While one-shot transactions predominate the mass-market sale of goods, Article 2 covers long-term requirements or output contracts.

As Diagram One reveals, there is little overlap between the attributes of sale of tangibles and licensing of intangibles. The licensing of an Internet security product is based upon entirely different assumptions than is an Article 2 sale. While courts have attempted to stretch Article 2 to accommodate the licensing of intangibles, the principles of Article 2 do not correspond to the commercial reality of licensing transactions in most significant respects. For example, the performance obligations of a buyer under Article 2 are a poor match for the obligations of a licensee, as are warranties under Article 2.²⁹⁶ Article 2 remedies are also ill-equipped to address licensing transactions. There is uncertainty whether a software licensor has the right to include a disabling device in its program as the functional equivalent of self-help repossession. Article 2 allows a buyer to reject the whole product if it fails "in any respect to conform to the contract."²⁹⁷ Would this "perfect tender rule" of Article 2 permit a licensee to reject a program arbitrarily because it contains a few lines of errant code? The mass-marketing of some Internet security software applications most closely resembles the sale of goods, but even here there are significant differences. For example, goods under U.C.C. sales law are freely assignable, whereas licensors typically attempt to restrict assignability. This is far afield from an Article 2 sale.

There is a great deal of uncertainty as to how, or if, courts could reconcile U.C.C. sales principles with the licensing of Internet security products. Article 2 does not address such fundamental issues as the enforceability of shrink-wrap licensing, warranty disclaimers, third-party rights and appropriate remedies for the breach of a license agreement. Without clear rules, there will be uncertainty in the allocation of risk in Internet security contracts.

296. In the sale of goods, a buyer is expected to accept or reject goods promptly. However, a licensee may need more time to reject non-conforming software products. Many customized licenses provide for an "acceptance testing period." However, § 2-602(1) states that the rejection must be "within a reasonable time after their delivery or tender." U.C.C. § 2-602(1) (1990). Should a licensee be deemed to have a "reasonable opportunity" for acceptance testing? Section 2-602(1) provides only a "reasonable opportunity to inspect" the goods. *Id.* This doctrine seems inapplicable to complex computer contracts where acceptance testing may extend over a number of months. See *Beasley Ford, Inc. v. Burroughs Corp.*, 361 F. Supp. 325 (E.D. Pa. 1973), *aff'd*, 493 F.2d 1400 (3d Cir. 1974) (holding that eight months was not an unreasonably long time given the complexity of a computer).

Under Article 2 sales, no implied warranties are contemplated for "system integration," "confidentiality of data," or "data integrity." See U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995).

297. U.C.C. § 2-601 (1990).

IV. REGULATION OF INTERNET SECURITY PRODUCTS UNDER PROPOSED U.C.C. ARTICLE 2B

The importance of security software and other intangibles to the National Information Infrastructure and to our economy cannot be underestimated. The regulation of transactions involving intangibles, such as security software, requires a specialized body of law that balances the competing interests of consumers and stakeholders in the software industry. Current law has proven inadequate for this purpose. Article 2 does not even address the licensing of intangibles, which is not surprising since the U.C.C. was completed in 1951, decades before the rise of software, telecommunications services and multimedia entertainment services. Due to the inadequacies of existing law, forging a contract law for intangibles has become a top priority in the revision of the Uniform Commercial Code.²⁹⁸ The result is Article 2B, the proposed software licensing law. Article 2B has the potential to modernize the general licensing of intangibles like security software. Part IV of this article advocates the adoption of the proposed Article 2B as a comprehensive legal framework for regulating the licensing of security software and other transactions involving intangibles.

At the time of the writing of this article, a draft of Article 2B is not available for public review; it is, however, scheduled to be available in early 1996. The earliest that Article 2B will be approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) is the summer of 1996.²⁹⁹ NCCUSL appointed Raymond T. Nimmer to draft the new article.³⁰⁰ Professor Nimmer co-drafted Article 2B's ill-fated predecessor—the "hub and spoke" paradigm for Article 2.³⁰¹ Since it is likely that much of the law

298. See Amelia H. Boss, *Developments on the Fringe: Article 2 Revisions, Computer Contracting, and Suretyship*, 46 BUS. LAW. 1803 (1991); Jeffrey B. Ritter, *Software Transactions and Uniformity: Accommodating Codes Under the Code*, 46 BUS. LAW. 1825 (1991) (describing U.C.C. revision project to incorporate software into Article 2).

299. Future drafts of the software licensing article will be available from the Commission. The Commission's address and telephone number are: National Conference of Commissioners on Uniform State Laws, 676 North St. Clair Street, Suite 1700, Chicago, IL 60611; (312) 915-0195. Copies of the Sept. 10, 1994 discussion draft are available from Chicago-Kent Law School's site on the World Wide Web, "<http://www.kentlaw.edu/ulc/>."

300. Thom Weidlich, *Commission Plans New U.C.C. Article*, NAT'L L. J., Aug. 28, 1995, at B1. Raymond Nimmer, a professor of law at the University of Houston, is a well-known legal academic and computer law practitioner. See Raymond T. Nimmer, *Intangibles Contracts: Thoughts of Hubs, Spokes, and Reinvigorating Article 2*, 35 WM. & MARY L. REV. 1337 (1994).

301. In March of 1995, NCCUSL approved a "hub and spoke" paradigm for the reconstruction of Article 2. The "hub and spoke" arrangement assumed that all

developed in the "hub and spoke" will be tracked quite closely in Article 2B,³⁰² this article uses the "hub and spoke" draft as a prototype for discussing the new software licensing law.

Article 2 transactions share general principles of law such as contract formation, unconscionability and the statute of frauds. See UNIFORM COMMERCIAL CODE: REVISED ARTICLE 2, (Proposed "Hub and Spoke" Draft, Feb. 10, 1995) (Raymond Nimmer, Reporter). The "hub" of Article 2 consisted of the general principles which were to apply to discrete chapters or "spokes" of Article 2, such as sales, leases or licenses.

The "hub and spoke" model was opposed from the beginning by software stakeholders. Drafts of the "hub and spoke" licensing chapter were circulated to diverse groups including the Software Publishers' Association, Business Software Alliance, Information Industry Association, Software Coalition, AIPLA, ABA Business Law Section, ABA Section on Intellectual Property, ABA Section of Science and Technology, Licensing Executives Society, Computer Law Association and local Bar associations. See generally Corinne Cooper, *The Madonnas Play Tug of War with the Whores or Who Is Saving the U.C.C.?*, 26 LOY. L.A. L. REV. 563 (1993) (arguing that the U.C.C. revision process must be vigilant and must not be captured by special interest groups); Edward L. Rubin, *Thinking Like a Lawyer, Acting Like a Lobbyist: Some Notes on the Process of Revising U.C.C. Articles 3 and 4*, 26 LOY. L.A. L. REV. 743 (1993) (describing the interest group politics of U.C.C. revision).

The Software Publishers Association (SPA) expressed early opposition to the "hub and spoke" paradigm. The SPA claimed that "[e]xcept for [two people], no one on the 16-member drafting committee working on Article 2 of the U.C.C. seems to have any experience in licensing, high-technology matters, and intellectual property." Groner, *supra* note 288, at 1. The SPA also criticized the draft as being skewed in favor of the consumer. *Id.* An in-house attorney for a Fortune 500 firm contended that the Article 2 drafters are "pro-buyer" and "anti-seller." *Id.* (quoting Norman Rosen, Counsel to General Electric). Norman Rosen attributed much of the pro-consumer bias to the composition of the drafting committee: "Many of the law professors on the panel have a pro-consumer bias, or are liberals." *Id.*

The "hub and spoke" paradigm was also critiqued "by several representatives of the software industry and Bar, and by some commercial law scholars." Thomas J. McCarthy, Corporate Counsel, DuPont Legal, Chair of the ABA Business Law Section Task Force on the Revision of Article 2, *NCCUSL Article 2 Drafting Committee: October 14-16, 1994 Meeting*, Oct. 21, 1994, at 1. The Computer Law Committee of the Association of the Bar of the City of New York concluded that the Draft should consider "eliminating the 'hub and spoke' structure." Letter from Ronald Abramson, Committee Chair, The Association of the Bar of the City of New York, Committee on Computer Law, to National Conference of Commissioners on Uniform State Laws 7 (Oct. 7, 1994) (on file with author). Some argued that intangible licensing has little in common with the "sale of goods." Zan Hale, *U.C.C. Article 2 Drafting Committee Faces Critics*, CORP. LEGAL TIMES, Oct. 1994, at 24.

The death knell of the "hub and spoke" paradigm was sounded in August of 1995 when NCCUSL abandoned the model of a "hub and spoke" in favor of a stand-alone software article [hereinafter proposed Article 2B]. See generally Weidlich, *supra* note 300, at B1 (reporting that NCCUSL rejected the restructuring of the U.C.C. in the "hub and spoke"). Many of the legal doctrines for resolving software issues developed in the "hub and spoke" will be reformulated in the separate software article.

302. We do not suggest that there is as yet an engineered consensus on controversial issues such as the content of performance warranties, remedies, or the enforceability of shrink-wrap licenses. New Article 2B, like its predecessor, will also be revised by the U.C.C. revision process. However, the fact that Raymond Nimmer, drafter of the

In addition to Professor Nimmer (Article 2B's "Technology Reporter"), the key players in the formation of Article 2B are: the American Bar Association (ABA),³⁰³ the NCCUSL³⁰⁴ and the American Law Institute (ALI).³⁰⁵ However, what should or should not be incorporated within the scope of Article 2B is a subject of much debate. For example, lawyers representing large commercial buyers of network systems favor remedies which provide them with assurance that consequential damages will be recouped. If a vendor of an Internet security product represents that its product insures "bullet-proof security" and that system fails due to the licensor's fault, the licensee will want to recover consequential damages.³⁰⁶

licensing chapter of the "hub and spoke," was reappointed to draft the separate article provides a strong indication Article 2B will share much common ground with the abandoned "hub and spoke."

303. The Software Contracting Subcommittee of the Uniform Commercial Code Committee of the Business Law Section of the American Bar Association has been a key player in the drafting of the software licensing provisions. The Subcommittee is chaired by Donald A. Cohn, Senior Counsel of DuPont, and Ellen Kirsh, Vice President and General Counsel of America Online. The Subcommittee is composed of corporate counsel, experienced software lawyers, computer law practitioners, legal academics and consumer representatives. The Subcommittee has engaged in a number of projects. One of the tasks has been to analyze and provide comments to the NCCUSL about the issuance of the "hub and spoke" draft. The Subcommittee's work reflects an ABA position on the proposed draft. The Subcommittee also coordinates with other ABA sections such as Intellectual Property and Law and Technology. The Subcommittee provides the Technology Reporter with issue papers.

Since 1992, the Subcommittee has also been divided into working groups. Michael Rustad, co-author of this article, has been a Task Leader for third-party and scope issues and was appointed Co-Chair of the Task Force on General Provisions of the Proposed U.C.C. Article 2B on the licensing of intangibles in September of 1995.

304. Along with the American Law Institute, the NCCUSL approves proposed drafts and votes on whether to submit a completed draft to state legislatures. NCCUSL appointed the Technology Reporter and the drafters of revised Article 2.

305. The American Law Institute of Philadelphia, Pennsylvania is a key sponsoring organization for the Code. Stephen C. Veltri & Ronald S. Gross, *Introduction to the Uniform Commercial Code Survey: The Role of the Courts in a Time of Change*, 49 BUS. LAW. 1827, 1830 (1994). The ALI was the promulgator of the influential Restatements and most other successful codification projects. Its membership is composed of distinguished practitioners, judges and legal academics. Dom Calabrese et al., *Karl Llewellyn's Letters to Emma Cortsvet Llewellyn from the Fall 1941 Meeting of the National Conference of Commissioners on Uniform State Laws*, 27 CONN. L. REV. 523, 525 (1995).

306. Consequential damages are recoverable under § 2-715(2) of current Article 2. Recovery of consequential damages provides recovery for losses beyond the basic damages recovery found in § 2-714. The failure of Internet security may result in realized losses, economic loss, or even personal injury. An attorney for Consumers Union believes that software contracts should offer the same protection as do contracts in the sale of goods: "Customers expect the product to work. When you open the box, it's just like a toaster. If that's not the business you're in, you'd better make it clear." Groner, *supra* note 288, at 26.

In order to learn more about what practitioners would like incorporated within the scope of Article 2B, co-author Michael Rustad surveyed the membership of the Computer Law Association (CLA Survey).³⁰⁷ The CLA Survey's goal was to collect data on the extant and emergent software licensing law by querying lawyers who work in this field.³⁰⁸ The quantitative findings of the CLA Survey are reproduced in Appendix B. Some of the results are also described in the text to give the reader an idea of practitioners' concerns.³⁰⁹

This part is divided into two subparts. Subpart IV.A. discusses each section of the proposed Article 2B—in order to appreciate the effective, coherent legal regime afforded by Article 2B, it is necessary to first understand its basic provisions—and discusses Article 2B's effect on mass-market licenses. Subpart IV.B. presents our case for adopting Article 2B for regulating transactions involving Internet and network security software.

307. This empirical study was conducted in the Fall of 1994. The Computer Law Association (CLA) membership consists of intellectual property lawyers who develop, distribute and use computer technology. We designed a national survey on the computer law practitioner's view of software licensing issues as well as the proposed licensing chapter of Article 2 of the U.C.C. The instrument was field tested in the Summer of 1993. This survey was mailed to all 950 North American members of the CLA in August of 1994.

We received 147 responses to the survey which represented a 15% response rate. Members of the CLA responding to our survey represented an excellent cross-section of lawyers working with software law. Respondents were from 29 states, the District of Columbia and Canada. The majority of respondents were from Massachusetts, California, the District of Columbia, Virginia and New York. The respondents were 86% male and 14% female. The sample reflected a reasonable balance between attorneys who represented vendors and buyers. The vast majority of these computer lawyers had five or more years of software legal experience. Our sample included representatives of diverse branches of the software industry, including on-line providers as well as large-scale users from the general corporate community. In the CLA Survey's second section, respondents were asked to state their agreement with statements concerning various aspects of software law. Topics surveyed were the definition of mass-marketed software, assignability, warranty, disclaimers, shrink-wrap licenses and scope of rights. The third section presented five software legal hypotheticals and asked how licensing law should resolve the issues raised by each scenario. The final section surveyed respondents' awareness and attitude toward the software "spoke" of proposed revisions to Article 2 of the U.C.C. See Michael Rustad et al., *An Empirical Analysis of Software Licensing Law and Practices (Part Two)*, 10 (4) COMPUTER L. ASS'N BULL. 3 (1995).

308. *Id.*

309. Throughout this part, we cite to specific comments of some CLA respondents. Anecdotal comments made by respondents were assured the same privacy and confidentiality as their completed CLA surveys. All surveys, including respondents' unstructured comments as quoted within this article, are on file with co-author Michael Rustad.

A. Anatomy of Proposed U.C.C. Article 2B

The proposed Article 2B will likely consist of six parts: (1) General Provisions; (2) Formation and Construction; (3) Performance and Construction; (4) Warranties; (5) Effect of License on Third Parties; and (6) Default and Remedies.³¹⁰ We will discuss each part in turn, detailing the likely provisions and providing practitioners' perspectives on each topic based on the results of the CLA Survey. We will also discuss the controversy surrounding Article 2B's treatment of mass-market licenses.

1. GENERAL PROVISIONS

The general provisions section of Article 2B will likely contain definitions previously located in both the "hub" and "spoke" provisions for intangibles.³¹¹ The proposed licensing article will reconcile the "hub" and "spoke" sections in a stand-alone article which will include terminology applicable to the licensing of security software. The proposed Article 2B will apply to "intangible contracts and agreements incidental to intangible contracts"³¹² and will encompass concepts such as the mass-market license,³¹³ "intangible,"³¹⁴ "consumer contracts,"³¹⁵ "record,"³¹⁶ and "signed."³¹⁷ Similarly, the new software licensing article will quite likely validate electronic contract formation by exchange of records.³¹⁸

One of the key general provisions will be the definition of "intangibles." As in the "hub and spoke" draft, intangibles will be defined as "data, information, software and any intellectual property rights associated with the data, information, or software, whether or not the intangible is embodied in tangible form."³¹⁹ The provisions

310. These six parts correspond to the main elements of the "hub and spoke" paradigm.

311. The General Provisions of the "hub and spoke" draft covered definitions, scope, choice of law and transfer of rights provisions. U.C.C., Rev. Article 2 (Proposed "Hub and Spoke" Draft, Feb. 10, 1995) (Raymond Nimmer, Reporter).

312. U.C.C. § 2-102(a) (Proposed Draft, Feb. 10, 1995). Under the proposed Article 2B, the following will specifically be *excluded* from U.C.C. treatment: 1) patents; 2) trade secrets; 3) know-how or similar intangibles unrelated to software or a computer program; and 4) embedded software (*e.g.*, PROM in a pickup truck). *See, e.g.*, U.C.C. § 2-2102(C) (Proposed Draft, Feb. 10, 1995).

313. *See, e.g.*, U.C.C. § 2-2101(1) (Proposed Draft, Feb. 10, 1995).

314. *See, e.g.*, U.C.C. § 2-102(a)(27) (Proposed Draft, Feb. 10, 1995).

315. *See, e.g.*, U.C.C. § 2-102(a)(12) (Proposed Draft, Feb. 10, 1995).

316. *See, e.g.*, U.C.C. § 2-102(a)(39) (Proposed Draft, Feb. 10, 1995).

317. *See, e.g.*, U.C.C. § 2-102(a)(42) (Proposed Draft, Feb. 10, 1995).

318. *See, e.g.*, U.C.C. § 2-102(a)(22) (Proposed Draft, Feb. 10, 1995).

319. U.C.C. § 2-102(a)(27) (Proposed Draft, Feb. 10, 1995).

will probably also use a definition of an "intangible contract" similar to that used in the "hub and spoke" version: "a license, software contract, continuous access contract or other agreement to transfer rights in intangibles."³²⁰ Thus, the licensing of security software, such as an anti-virus program, would qualify as an "intangible contract." The proposed Article will probably incorporate the "hub and spoke" definition of "computer program": "a set of statements or instructions" that is "capable of causing a machine having information processing capabilities to indicate, display, perform or achieve a function or result."³²¹ Security software fits this definition.³²² Furthermore, the licensing of security software is a method of transferring rights that will be validated by the proposed general provisions.³²³ The proposed Article 2B's definitions will provide the appropriate legal infrastructure for approaching and managing the licensing of security software.

2. FORMATION AND CONSTRUCTION

The hallmark of Article 2 contract formation, which the proposed Article 2B will likely incorporate, is its flexibility and realism. Article 2's section 2-204, for example, is a liberal formation rule, requiring only that formation be "sufficient to show agreement."³²⁴ The U.C.C. permits a contract for sale of goods to be formed even though one or more of its terms are left open, as long as a reasonably certain basis exists for a court to grant an appropriate remedy in the event of breach.³²⁵ Like Article 2's default terms for sales transactions,³²⁶ the proposed Article 2B will likely provide

320. U.C.C. § 2-102(a)(28) (Proposed Draft, Feb. 10, 1995).

321. U.C.C. § 2-102(a)(8) (Proposed Draft, Feb. 10, 1995).

322. Security software is essentially a set of instructions that causes a computer to achieve the function of excluding intruders or protecting confidentiality. Security is the task or result of the software program. Thus, the intangible instructions of security software will be easily accommodated in Article 2B.

323. The "hub and spoke" draft defined the "license" as "an agreement for a transfer of rights in an intangible where the rights transferred are conditional or limited, whether or not the agreement provides for delivery of tangible property that contains the intangible. The term does not include the reservation or creation of a security interest in an intangible." U.C.C. § 2-102(30) (Proposed Draft, Feb. 10, 1995).

324. U.C.C. § 2-204(1) (1990).

325. U.C.C. § 2-204(3) (1990). Additionally, section 2-206 supplements sections 2-204 and 2-205 in setting forth how a contract is formed under Article 2. Section 2-206(1)(b), for example, provides that an "order for prompt shipment . . . invites acceptance by a prompt promise to ship or by prompt shipment." U.C.C. § 2-206(1)(b) (1990).

326. See U.C.C. §§ 2-305 to -311 (1990) (affixing default provisions relating to price, output and requirement contracts; method, place and time of delivery; time and method of payment; and assortment of goods).

default, general obligation gap-fillers appropriate to the licensing of intangibles.

The presumption of confidentiality, for example, would be a gap-filler where the intangible contract is silent.³²⁷ Other key gap-fillers in the proposed Article 2B will include scope of the license, number of users, number of machines, scope of the grant of the license and time of license creation.³²⁸ In addition, licensees will not be automatically entitled to developments or modifications of software in the absence of agreement,³²⁹ nor will they be deemed to have a right to an intangible's underlying data or source code³³⁰ unless the license expressly grants that right.³³¹ Article 2B will likely also define default rules for location and use restrictions. In the absence of agreement to the contrary, a licensee of Internet security software will be able to use the product in any location that is reasonable.³³² If a licensee exceeds the scope of use restrictions, it will be in breach.³³³ Thus, the proposed Article 2B's gap-filler provisions will directly

327. *See, e.g.*, U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

328. The proposed Article 2B will probably provide the gap-filler that a license is non-exclusive, meaning that a licensee will only have the right to use a single copy of the software at a single time, on a single machine. *See, e.g.*, U.C.C. § 2-2204(a) (Proposed Draft, Feb. 10, 1995). Of course, the parties will be free to negotiate around these provisions. Another Article 2B gap-filler will be the definition of "all rights" or "all uses" of a license to cover all future uses. *See, e.g.*, U.C.C. § 2-2204(b)(1) (Proposed Draft, Feb. 10, 1995). Similarly, the proposed Article will likely cover all rights necessary to use rights transferred by the license agreement. *See, e.g.*, U.C.C. § 2-2204(b)(2) (Proposed Draft, Feb. 10, 1995).

329. *See, e.g.*, U.C.C. § 2-2205 (Proposed Draft, Feb. 10, 1995). However, if a vendor does grant its customer software enhancements, the contract term will likely be defined by reasonableness and industry standards. *Id.*

330. Many software licensing contracts specify that only object code will be supplied to the licensee and that the source code will remain with the licensor. This is because the distribution of the source code may jeopardize its status as a trade secret. A computer program is generally written in an easily understood programming language. This is referred to as "source code." This source code must be translated into corresponding machine-readable instructions. The resulting set of instructions is referred to as "object code" and is, as a practical matter, unintelligible to anything but the machine for which it is designed. The source code and object code are treated as one for copyright purposes. "Because the object code is the encryption of the copyrighted source code, the two are to be treated as one work; therefore copyright of the source code protects the object code as well." *GCA v. Chance*, 217 U.S.P.Q. (BNA) 718 (1982).

331. *See, e.g.*, U.C.C. § 2-2206 (Proposed Draft, Feb. 10, 1995). As a result of this gap-filler, an on-line security provider, such as America Online, would not have to hand over the underlying data on its system unless this access was specified in the contract.

332. *See, e.g.*, U.C.C. § 2-2208 (Proposed Draft, Feb. 10, 1995).

333. *Id.* A breach would also occur if the licensee exceeded the designated number of copies of a software program. *See id.*

respond to the realities of Internet security software licensing transactions.

3. PERFORMANCE AND CONSTRUCTION

The proposed Article 2B's "Performance and Construction" part will likely include tender, acceptance, rejection and revocation provisions. The net effect of these provisions will be to provide a framework of general construction and performance principles which accord with the commercial reality of licensing intangibles transactions, and thus security software transactions. Each provision will be discussed in turn.

a. Tender and Acceptance

Under Article 2, the delivery of goods triggers the buyer's duty "to accept and pay in accordance with the contract."³³⁴ The proposed Article 2B will likely replace the concept of "delivery" with that of "transfer of rights." A transfer of rights will consist of the "grant of a right to have access to, modify, disclose, distribute, copy, use, have used on behalf of the transferee, or otherwise take action with respect to an intangible coupled with any actions necessary to enable the transferee to exercise those rights."³³⁵ Under the proposed Article 2B, the licensor's tender will thus occur upon the transfer of rights to the intangibles,³³⁶ by either physical delivery or electronic means.³³⁷ Similarly, the licensee's tender of payment may be made through physical, electronic or any other reasonable means.³³⁸

With respect to tender, Article 2 employs the "perfect tender rule," affording an aggrieved buyer the option to reject goods "if the goods or the tender of delivery fail in any respect to conform to the contract."³³⁹ However, this logic fails in the context of security software licensing because "minor flaws ('bugs') are common in virtually all software."³⁴⁰ Under a perfect tender rule licensees would be able to routinely reject the "flawed" software since it would probably not conform to the licensing agreement. To correct this, the

334. U.C.C. § 2-301 (1990).

335. U.C.C. § 2-102(a)(51) (Proposed Draft, Feb. 10, 1995).

336. *See, e.g.*, U.C.C. § 2-2104 (Proposed Draft, Feb. 10, 1995).

337. *See, e.g.*, U.C.C. §§ 2-2301, 2-2302 (Proposed Draft, Feb. 10, 1995).

338. *See, e.g.*, U.C.C. § 2-2303(b) (Proposed Draft, Feb. 10, 1995).

339. U.C.C. § 2-601 (1990).

340. U.C.C. § 2-2106 cmt. 6 (Proposed Draft, Sept. 10, 1994).

proposed Article 2B will likely replace the perfect tender rule with a "substantial performance" standard.³⁴¹

The relational or ongoing nature of software licensing contracts lends additional support for a substantial performance standard. Some security software has a period of "acceptance testing" in which minor bugs are fixed. Other transactions involve a maintenance contract or provide updates as a program is improved. Unstructured interviews conducted as part of the CLA Survey revealed that most attorneys favor the substantial performance standard rather than the perfect tender rule.³⁴²

b. Rejection and Revocation

As with Article 2, a software licensee under the proposed Article 2B will likely have a flexible array of options upon the licensor's improper tender, including rejection³⁴³ and revocation.³⁴⁴ These provisions are discussed more fully in part 6, in the context of defaults and remedies.

4. WARRANTIES

The legal structure for security software must resolve the issues of express and implied warranties and the clauses that attempt to limit damages. The proposed Article 2B's warranty provisions will probably closely fit the realities of security software. The CLA Survey indicated that the lack of uniform warranty standards for software licensing constituted one of the primary arguments for codification.³⁴⁵ One attorney wrote, "Throughout the country, these

341. See, e.g., U.C.C. § 2-2306 (Proposed Draft, Feb. 10 1995). The substantial performance standard does not mean, however, that minor flaws will be tolerated. Dean Nimmer states:

A substantial performance rule does *not* hold that substantial (but imperfect) performance of a contract is not a breach. To the contrary, both the common law and the rule here treat substantial (but imperfect) performance as a breach of contract. The significance of the concept of substantial performance lies in the remedy available to the injured party. Unless a breach is material, it cannot be used as an excuse to void or avoid the contract obligation. A licensee who receives substantial (but imperfect) performance from the licensor, cannot reject the initial tender or cancel the contract on that account, but it can obtain financial satisfaction for the less than complete performance.

U.C.C., Rev. Article 2, Sales, Chapter 3: Licenses, Prefatory Note 9 (Proposed Draft, Sept. 10, 1994) (Raymond Nimmer, Reporter).

342. CLA Survey, *supra* note 307.

343. See, e.g., U.C.C. § 2-2306(a) (Proposed Draft, Feb. 10, 1995).

344. See, e.g., U.C.C. § 2-2311 (Proposed Draft, Feb. 10, 1995).

345. CLA Survey, *supra* note 307.

are resolved differently depending on the jurisdiction. Uniform rules would be extremely helpful in this area."³⁴⁶ This part will discuss how the proposed Article 2B will likely address both express and implied warranties, as well as disclaimers and limitations of such warranties.

a. Express Warranties

The proposed Article 2B's express warranty provisions for software licensing will probably be substantially similar to those presently provided for the sale of goods under Article 2.³⁴⁷ For example, affirmations of fact which form part of the "basis of the bargain" will likely become part of the agreement between the parties at the time of initial transfer of rights.³⁴⁸ However, if mass-marketed information or data is the subject of the transfer, there will likely be no warranty of accuracy in the information without an express warranty to a specific licensee.³⁴⁹ A developer of pre-packaged software who gives written warranties to consumers will not only be subject to the provisions of the proposed Article 2B, but will also likely be subject to the federal Magnuson-Moss Act.³⁵⁰

346. *Id.*

347. The methodology for creating express warranties for software licensing is substantially similar to the law of sales. A licensor of security software could create express warranties through samples, models, demonstrations or descriptions. Words such as "warranty" or "guaranty" will be unnecessary. The sole test of an express warranty in a software licensing transaction will be whether the statement constitutes part of the basis of the bargain. Compare U.C.C. § 2-2402 (Proposed Draft, Feb. 10, 1995) with U.C.C. § 2-313 (1990). See, e.g., *infra* App. A § 14.

348. See, e.g., U.C.C. § 2-2402(a)(1) (Proposed Draft, Feb. 10, 1995).

349. See, e.g., U.C.C. § 2-2402(c) (Proposed Draft, Feb. 10, 1995).

350. The Magnuson-Moss Warranty—Federal Trade Commission Improvement Act provides remedies for consumers against all warrantors of products. 15 U.S.C. § 2301, 88 Stat. 2183 (1975). It defines a consumer as follows:

The term "consumer" means a buyer (other than for purposes of resale) of any consumer product, any person to whom such product is transferred during the duration of an implied or written warranty (or service contract) applicable to the product, and any other person who is entitled by the terms of such warranty (or service contract) or under applicable State law to enforce against the warrantor (or service contractor) the obligation of the warranty (or service contract).

15 U.S.C. § 2301(3) (1975).

Suppliers are subject to Magnuson-Moss warranties. A "supplier" is any person selling consumer products. 15 U.S.C. § 2301(4) (1975). A "warrantor" is any supplier who gives a written warranty or who is obligated under an implied warranty. 15 U.S.C. § 2301(5) (1975). The Magnuson-Moss Warranty Act provides rules for two types of written warranties, full and limited. Full warranties are described in 15 U.S.C. § 2304 (1975). A full warrantor must give a consumer a full refund or replacement without charge after a product fails and after a reasonable number of

b. Implied Warranties

Implied warranties for software licensed under the proposed Article 2B will likely be quite different than implied warranties for goods under Article 2. Nevertheless, Article 2's implied warranty of "merchantability"³⁵¹ and implied warranty of "fitness for a particular purpose"³⁵² will likely have their functional equivalents in the proposed Article 2B. These will be the implied warranty of quality³⁵³ and the implied warranty of system integration,³⁵⁴ respectively. The proposed Article will probably create two other implied warranties, an electronic security warranty³⁵⁵ and an implied warranty for information and services.³⁵⁶ The implied warranties for electronic security and system integration will be specifically tailored to the licensing of intangibles. The implied warranty for system integration³⁵⁷ would apply where the licensee relies upon the licensor's expertise to make the software suitable for the licensee's purposes. When the licensee's reliance is disclosed by the contract, or from other circumstances, the licensor will likely be subject to an implied warranty of "reasonable care" and "workmanlike effort" to achieve the licensee's purposes.³⁵⁸ Moreover, if the product is an integrated system, the licensor will likely be further subject to the

attempts at repair. Consumers may obtain damages, legal, or equitable relief under the act. See 15 U.S.C. § 2310(d) (1975).

Assuming that security software is sold to a consumer and "written warranties" are given, Magnuson-Moss would likely apply. A consumer damaged by the failure of Internet security software may bring suit "for damages and other legal and equitable relief." 15 U.S.C. § 2310(d)(1) (1975). The Magnuson-Moss Warranty Act would permit a dissatisfied licensee to recover attorney's fees "as part of the judgment." 15 U.S.C. § 2310(d)(2) (1975). Assuming Magnuson-Moss applied to mass-marketed security software, the Federal Trade Commission (FTC) rules for warranties would also apply. 40 Fed. Reg. 60188 (1975) (codified at 16 C.F.R. § 701) The FTC rules also provide for informal dispute settlement. 40 Fed. Reg. 60215 (1975) (codified at 16 C.F.R. § 703).

351. See U.C.C. § 2-316 (1990).

352. U.C.C. § 2-315 (1990).

353. See, e.g., U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995). Non-data items of a transaction, such as protective "boot disks" for laptop computers, will be subject to the implied warranty standard of "substantial conformance." See, e.g., U.C.C. § 2-2403(a) (Proposed Draft, Feb. 10, 1995).

354. See, e.g., U.C.C. § 2-2405(c) (Proposed Draft, Feb. 10, 1995).

355. See, e.g., U.C.C. § 2-2406 (Proposed Draft, Feb. 10, 1995).

356. See, e.g., U.C.C. § 2-2404 (Proposed Draft, Feb. 10, 1995). Information and services components of a software licensing transaction will be governed by the implied warranty standard of "reasonableness and workmanlike effort." See, e.g., U.C.C. § 2-2404(a) (Proposed Draft, Feb. 10, 1995).

357. See, e.g., U.C.C. § 2-2405 (Proposed Draft, Feb. 10, 1995).

358. See, e.g., U.C.C. §§ 2-2405(a), (b) (Proposed Draft, Feb. 10, 1995).

implied warranty that its components "will function together as a system substantially consistent with the goals of the licensee."³⁵⁹

The implied warranty for electronic security will be applicable to the transfer of rights by electronic access.³⁶⁰ This implied warranty will require the licensor *and* the licensee to use reasonable care to exclude: 1) unauthorized access by third parties; 2) undisclosed programs; and 3) extraneous data.³⁶¹ The standard will probably be the same as that used in the "hub and spoke" version—whether the allowance or inclusion of the above could "reasonably be expected to damage data, software systems, or operations."³⁶²

c. Disclaimers and Limitations

Under Article 2, a disclaimer occurs when a seller of goods uses language or conduct to negate or limit implied warranties.³⁶³ Disclaiming warranties under the proposed Article 2B will likely parallel Article 2's provisions with two notable exceptions: 1) the "writing" requirement for modification or exclusion of warranties may expressly be met by means of an electronic record;³⁶⁴ and 2) any exclusion with regard to a *consumer* will be *inoperative* unless the consumer "expressly" consents.³⁶⁵ However, while reasonable disclaimers will likely be permitted,³⁶⁶ unconscionable disclaimers will not be enforced, nor will remedies that fail of their essential purpose.³⁶⁷

In the CLA Survey, computer lawyer respondents were asked for their opinion on how to resolve warranty issues for the licensing of intangibles. The extent to which the proposed Article 2B should permit vendors to disclaim or limit liability was a subject of great controversy in the CLA Survey. Article 2 already permits vendors to disclaim implied warranties by conspicuous use of terms such as "with all faults" or "as is."³⁶⁸ One respondent representing a large-scale

359. U.C.C. § 2-2405(c) (Proposed Draft, Feb. 10, 1995).

360. *See, e.g.*, U.C.C. § 2-2406 (Proposed Draft, Feb. 10, 1995).

361. *See id.*

362. *Id.*

363. *See* U.C.C. § 2-316 (1990). For an example of such a disclaimer, *see* App. A § 14, *infra*.

364. *See, e.g.*, U.C.C. § 2-2407(b) (Proposed Draft, Feb. 10, 1995).

365. *Id.*

366. *See, e.g.*, U.C.C. § 2-2407 (Proposed Draft, Feb. 10, 1995).

367. *See, e.g.*, *Riley v. Ford Motor Co.*, 442 F.2d 670 (5th Cir. 1971) (exclusive remedy failed of its essential purpose when repeated car repair attempts were ineffective). *See also* *RRX Indus., Inc. v. Lab-Con, Inc.*, 772 F.2d 543, 547 (9th Cir. 1985) (holding that a disclaimer of consequential damages was unenforceable).

368. U.C.C. § 2-316(3)(a) (1990).

vendor argued that the law of software licensing "should permit a software vendor to contractually limit the end-user's remedy for breach of warranty to repair, replacement or refund."³⁶⁹ An attorney with a corporate law firm thought it important to clarify the extent that lost profits and consequential damages could be disclaimed.³⁷⁰ These issues arise in virtually every software performance dispute and Article 2B will likely provide a guide for resolving such issues.³⁷¹

5. EFFECT OF LICENSES ON THIRD PARTIES

a. Transfer of Title of Tangibles and Intangibles

Under Article 2, a buyer obtains title to the good, and power to transfer that title, when she pays the agreed price for the good.³⁷² In the software licensing context, a licensee obtains title to a copy of the intangible and may use that copy in any manner consistent with the licensing agreement.³⁷³ The proposed Article 2B will likely make clear that transfer of title to the copy (i.e., a copy of the software code) does not transfer title to the intangible (i.e., the software code), and therefore the licensee does not have power to transfer title to the intangible itself, unless this is explicitly agreed to and stated in the licensing agreement.³⁷⁴ Thus, the proposed Article 2B will essentially provide that a security software licensing agreement will determine the licensee's rights to transfer rights to a third party.³⁷⁵

b. Assignment of Licenses

The law of assignment must also be adjusted to accommodate the licensing of security software. The proposed Article 2B will likely codify the general rule that a licensee generally may not assign or

369. CLA Survey, *supra* note 307.

370. *Id.*

371. In general, the proposed Article 2B will probably treat licensing arrangements resembling the sale of goods as having product-quality warranties. *See, e.g.*, U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995). In contrast, a lesser warranty will likely be given for process-oriented transactions. *See, e.g.*, U.C.C. § 2-2404 (Proposed Draft, Feb. 10, 1995). This bifurcated warranty protection follows case law on sales and services. Warranties are generally provided for in sales, but not services. For a superb discussion of warranty issues in the proposed Article 2B, see Feldman, *New Draft*, *supra* note 264. *See also* Feldman, *Warranties*, *supra* note 274.

372. *See* U.C.C. § 2-301 (1990).

373. *See, e.g.*, U.C.C. § 2-2501 (Proposed Draft, Feb. 10, 1995); *infra* App. A § 6.

374. *See, e.g.*, U.C.C. § 2-2501 (Proposed Draft, Feb. 10, 1995); *infra* App. A § 13(b).

375. *Id.*

otherwise transfer a nonexclusive license.³⁷⁶ It will also provide that a licensor may freely assign his rights, provided the licensee's duties are not materially changed and the licensee's trade secrets and confidential information are not disclosed.³⁷⁷ In certain circumstances, a licensee will be able to assign her rights. A licensee may assign her rights in a license if "the license was a mass-market license, the licensee owned the copy of the intangibles, and the licensee transfers ownership of that copy and all other copies made by it pursuant to the license or applicable intellectual property law to its transferee."³⁷⁸

Many CLA Survey participants perceived assignability issues as a high priority for resolution in the proposed Article 2B.³⁷⁹ Data from the CLA Survey on third-party issues reveals industry consensus on an end-user's right to assign or resell software, irrespective of any shrink-wrap or other restrictions on assignment. Specifically, 83% of the computer lawyers surveyed agreed that "the law should allow the end-user to assign or resell software."³⁸⁰ A corporate counsel's

376. U.C.C. § 2-2502(a) (Proposed Draft, Feb. 10, 1995). This prohibition against assignment is at odds with many other U.C.C. articles that favor free assignability. See Edwin E. Smith, *Article 9 in Revision: A Proposal for Permitting Security Interests in Nonassignable Contracts and Permits*, 28 LOY. L.A. L. REV. 335, 338 (1994) (citing U.C.C. §§ 9-318(4), 2-210(2) and 2A-303 as examples of the free assignability norm). See, e.g., *infra* App. A § 20(f).

377. See, e.g., U.C.C. § 2-2502(b) (Proposed Draft, Feb. 10, 1995). This proposed section grants the licensor a right to assign rights under a license. However, if the assignment results in a hardship to the licensee, the licensor's transfer to the third party is prohibited. *Id.*

378. U.C.C. § 2-2502(a)(4) (Proposed Draft, Feb. 10, 1995). This provision comports with commercial realities since much security software resembles goods when it is mass-marketed and distributed over the Internet as "shareware" or "freeware." In such circumstances, consumers believe they "own" the software, and with ownership they expect that they are free to transfer ownership of the software, in the same sense as if the software was considered a good. Therefore, any contractual restrictions on such software are essentially inconsistent with the expectations of consumers (i.e., that they "own" the software).

379. The CLA Survey did not address issues involving the unauthorized transfer of copies of computer programs as copyright infringements. Software licenses generally allow the licensee to use the software for its own internal information processing. However, most licenses do not permit third parties to make "copies." Section 117 of the Copyright Act permits the "owner" of a copy of a computer program to make or authorize the making of another copy as an "essential step" in the use of the program or for "archival purposes." 17 U.S.C. § 117 (1994). Vendors usually argue that licensees who make other copies are infringing the licensor's copyright.

380. CLA Survey, *supra* note 307. However, most of the CLA respondents would place some limitation on the assignability of licenses. CLA Survey, *infra* App. B question 2. Most respondents agreed that an end user should have the right to move the physical location of software. Sixty-three percent agreed that a user should have the right to assign or resell software, irrespective of any shrink-wrap restrictions. Another 63% agreed that a licensee should have the right to assign software to an

view on assignment was typical of most responding intellectual property attorneys: "As long as the scope of use is not expanded by an assignment, the vendor should have little objection about assigning software. [The] licensor should have no objection about an outsourcer using software on behalf of "Company X" so long as scope of use is not altered."³⁸¹ The proposed Article 2B's provisions could go a long way toward resolving the difficult problems of assignability.

c. Copying, Use and Location Restrictions

Article 2B will probably follow its "hub and spoke" predecessor in providing that, if a software contract license grants the right to use a single or specified number of copies of the software,³⁸² the licensee's "making or retaining additional copies or permitting simultaneous use by multiple users" will be considered a breach, unless otherwise permitted by copyright law.³⁸³ Furthermore, if the licensor does not specify location limits, software may be used in any reasonable location.³⁸⁴ A majority of the CLA Survey respondents support these use and location restrictions.³⁸⁵

6. DEFAULT AND REMEDIES

The remedies for licensors and licensees under the proposed Article 2B will likely differ from Article 2 remedies currently available to sellers and buyers. For example, licensors will likely have a right to recover consequential damages under the proposed Article 2B,³⁸⁶ a remedy not accorded aggrieved sellers under Article 2.³⁸⁷ The remedies for licensors and licensees will be discussed in turn.

outsourcer (a firm hired to manage data processing activities). For mass-marketed software licenses, most respondents believed that software law should reflect the norm of free assignability.

381. CLA Survey, *supra* note 307.

382. Many software licenses specify the number of copies of a program that may be used at the same time or at a given site. The draft does not currently address the issue of whether software is in use when it exists in latent form on a hard drive or is it in use only when present in memory. In a multi-tasking machine, the same software may be loaded into different locations in memory at the same time. An unanswered question of the draft is whether each such copy constitutes a copy for purposes of the software license.

383. U.C.C. § 2-2208(c) (Proposed Draft, Feb. 10, 1995). *See also infra* App. A § 13(c)(ii).

384. *See, e.g.*, U.C.C. § 2-2208(a) (Proposed Draft, Feb. 10, 1995).

385. CLA Survey, *infra* App. B question 2.

386. *See, e.g.*, U.C.C. § 2-2610(c)(2) (Proposed Draft, Feb. 10, 1995).

387. *See, e.g.*, *infra* App. A § 15.

a. Licensor Remedies

In general, licensor remedies will likely turn on whether the nature of the licensee's default is material.³⁸⁸ If a licensee's breach is not material, the licensor may recover damages lost in the ordinary course of business.³⁸⁹ If a licensee's breach is material as to a part of the contract, the licensor may suspend its performance, recover damage to intangibles, recover damages lost for the particular performance, seek specific performance and recover the price.³⁹⁰ If a licensee's breach is material as to the entire contract, the licensor may cancel the contract, terminate rights, repossess and prevent further use, or recover damages as to the entire contract.³⁹¹

b. Licensee Remedies

The licensee's remedies for breach of the license contract by the licensor will also probably turn on whether the breach is material.³⁹² If the licensor's breach is not material, a licensee may not reject the performance as permitted under Article 2's "perfect tender" rule. An aggrieved licensee may, however, seek damages lost in the ordinary course of business, plus consequential damages, obtain recoupment, continue to use the intangibles, or exercise any remedies provided in the contract.³⁹³ If the licensor's default is material as to a part of the contract, the licensee would have the full array of remedies: rejection of the performance; revocation of acceptance; recovery of damages lost in the ordinary course of business; restitution or specific performance; recovery for damage to the value of its intangibles; or suspended performance demanding adequate assurances of performance.³⁹⁴ These same options are available for a licensor's material breach of the entire contract.³⁹⁵

7. MASS-MARKET LICENSES

The enforceability of mass-market licenses is a source of much confusion under current law. The proposed Article 2B will resolve this issue by defining different types of software licenses. Specifically, it will clarify and validate the differences between mass-marketed and

388. See, e.g., U.C.C. § 2-2515 (Proposed Draft, Feb. 10, 1995).

389. See, e.g., U.C.C. § 2-2521 (Proposed Draft, Feb. 10, 1995).

390. See, e.g., U.C.C. § 2-2610(b) (Proposed Draft, Feb. 10, 1995).

391. See, e.g., U.C.C. § 2-2610(a) (Proposed Draft, Feb. 10, 1995).

392. See, e.g., U.C.C. § 2-2603(a) (Proposed Draft, Feb. 10, 1995).

393. See, e.g., U.C.C. § 2-2603 (Proposed Draft, Feb. 10, 1995).

394. See, e.g., U.C.C. § 2-2603(b) (Proposed Draft, Feb. 10, 1995).

395. See, e.g., U.C.C. §§ 2-2603(a), 2-2603(d)(1) (Proposed Draft, Feb. 10, 1995).

customized software. Since various contract rules turn on whether a contract is mass-marketed, this is a critical distinction. The proposed software article will probably define a "mass-market license" as "a standard form license used in a retail or similar transaction in which the licensor does not modify the intangibles specifically for the transaction and the licensee does not sign a written license. The term includes a consumer license."³⁹⁶ This definition comports with the opinions of CLA Survey participants: an overwhelming majority of the respondents identified "mode of distribution" as an important criterion for distinguishing mass-market licenses from other licenses.³⁹⁷ It is also important to distinguish between one-shot transactions and relational contracts.³⁹⁸ Article 2B will recognize this distinction by identifying one-shot transactions as mass-market licenses, distinct from on-going and relational contracts.

The most common mass-market license is the "shrink-wrap"³⁹⁹ agreement. Licensors typically place a printed disclaimer of liability and limitation of remedies underneath the shrink-wrap, assuming that the licensee is bound upon opening the shrink-wrap.⁴⁰⁰ Most

396. U.C.C. § 2-2101 (Proposed Draft, Sept. 10, 1994). A "standard form" license is "a contract prepared by one party in advance for general and repeated use . . . substantially consisting of standard terms and actually used without negotiation of the standard terms with the other party." U.C.C. § 2-102(45) (Proposed Draft, Feb. 10, 1995).

397. Overall, 87% of the CLA Survey respondents agreed that the method of distribution was the best way to separate mass-marketed software from custom software. Sixty-five percent also viewed the form of the license agreement (i.e., shrink-wrap) to be a key criterion for distinguishing mass-marketed from service-oriented software. Additionally, 58% of the survey respondents agreed that the type of end user might also be important in defining mass-marketed software. Only 39% of the computer lawyers believed that mass-marketed software should be defined based upon the number of copies licensed. Only 28% of the respondents viewed price as the key criterion in distinguishing mass-marketed software. CLA Survey, Fall 1994 (*see infra* App. B question 1).

398. Relational contracts involve ongoing relationships where parties have repeat transactions, developing contracting rules through a course of dealing and performance. This ongoing relationship often discourages the parties from becoming involved in litigation. *See generally* Stewart Macaulay, *An Empirical View of Contract*, 1985 WIS. L. REV. 465 (1985). Stewart Macaulay, *Elegant Models, Empirical Pictures, and the Complexities of Contract*, 11 LAW & SOC'Y REV. 507 (1977). *Cf.* IAN MCNEIL, *THE NEW SOCIAL CONTRACT* (1980) (describing how parties employ nonlegal mechanisms to enforce relational contracts).

399. Shrink-wrap is the sealed plastic covering of a box containing software.

400. Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2318 n.26 (1994); Mark I. Koffsky, Note, *Patent Preemption of Computer Software Contracts Restricting Reverse Engineering: The Last Stand?* 95 COLUM. L. REV. 1160, 1166 (1995).

mass-marketed software is sold to consumers⁴⁰¹ in retail stores such as Egghead Software, Staples or CompUSA.⁴⁰² Under these conditions, the purchaser must adhere to the terms of the more powerful vendors. These standardized contracts become even more problematic as fewer players dominate the consumer market. Article 2B will account for the commercial reality that mass-marketed software licenses are seldom negotiated. Because requiring a signed and negotiated mass-marketed license agreement would vastly increase transaction costs, the proposed Article 2B will resolve the "unnegotiated" nature of mass-marketed software by validating a standard form license if a licensee—before or within a reasonable time after beginning to use the software—either expressly signs or manifests assent or has the opportunity to review the terms before manifesting assent.⁴⁰³ The emerging software licensing draft will thus conditionally legitimize the "standard form" license.

However, while the proposed Article may resolve the enforceability issue, the standard form license itself remains highly controversial. Merely breaking a shrink-wrap plastic sheet, even if the license terms are visible beforehand, does not connote any real agreement. It is a legal fiction to assume that consumers "agree" to a vendor's limitation of liability. Though there is little empirical research on the effectiveness of shrink-wrap in stemming unauthorized copying of software, it is apparent that shrink-wrap licensing has not solved the problem of unauthorized use.⁴⁰⁴ Moreover, mass-market licenses are presumed to be perpetual,⁴⁰⁵ whereas a non-mass-market license is terminable at will or with reasonable notice.⁴⁰⁶ Nevertheless, some states have enacted statutes providing for the enforcement of shrink-wrap software licenses.⁴⁰⁷ Even a shrink-wrap

401. The proposed Article will likely define both a "consumer" and a "consumer contract." See, e.g., U.C.C. §§ 2-102(11), (12) (Proposed Draft, Feb. 10, 1995) ("A 'consumer contract' means a contract for the sale or license of consumer property between a transferor regularly engaged in the business or selling or licensing and a consumer buyer.").

402. See, e.g., U.C.C. § 2-2101 (Proposed Draft, Feb. 10, 1995).

403. See, e.g., U.C.C. § 2-2203 (Proposed Draft, Feb. 10, 1995).

404. In the mid-1980s, unauthorized copying of software was widespread. One industry estimate was that there were anywhere between 2 and 10 unauthorized copies for every mass marketed software diskette purchased from the publisher. Page M. Kaufman, Note, *The Enforceability of State "Shrink-Wrap" License Statutes in Light of Vault Corp. v. Quaid Software, Ltd.*, 74 CORNELL L. REV. 222, n.2 (1988).

405. See, e.g., U.C.C. § 2-2210(a)(1) (Proposed Draft, Feb. 10, 1995).

406. See, e.g., U.C.C. § 2-2210(b) (Proposed Draft, Feb. 10, 1995).

407. See, e.g., LA. REV. STAT. ANN. § 51:1961-66 (Supp. 1981). During 1985, the state legislatures of California, Georgia and New York introduced but did not pass similar bills.

license which may be enforceable for purposes of contract law may collide with federal intellectual property law.⁴⁰⁸

Although the proposed Article 2B will likely run counter to recent trends against enforceability,⁴⁰⁹ it will only give effect to shrink-wrap agreements if the licensee is given reasonable procedural protection.⁴¹⁰ This strategy corresponds with the opinions voiced by CLA Survey respondents: 65% favored the enforceability of shrink-wrap licenses,⁴¹¹ and most advocated some procedural protection for mass-marketed software.⁴¹² Article 2B's validation of shrink-wrap licenses will clarify the law in favor of the vendor. Consumer advocates and many academics will find this resolution troubling, as it subordinates the interests of consumers to those of large commercial vendors.⁴¹³

408. Mark Lemley presents a compelling case against the enforceability of shrink-wrap licensing in the emergent software licensing law. Professor Lemley writes:

Shrinkwraps are not contracts at all in any meaningful sense of the word. Rather, they are unilateral lists of terms that courts may choose to abide by in some circumstances. Where the court must choose between a shrinkwrap term and creating its own term out of the air, perhaps there is reason to rely on the shrinkwrap But where there is already a federal statute in place that strikes a careful balance in the law, it would be a travesty to disregard that federal law because one party has indicated that it would prefer to have more rights than the law confers.

Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1291-92 (1995); see also Page M. Kaufman, *supra* note 404, at 222-23.

409. See, e.g., *Step-Saver Data System v. Wyse*, 939 F.2d 91, 105 (3rd Cir. 1991) (holding that, because a "box-top"—i.e., shrink-wrap—license agreement substantially altered the distribution of the risk between the buyer and the seller as a matter of law, it did not constitute a final and complete agreement between the parties). See generally Koffsky, *supra* note 400, at 1160.

410. For example, courts will not enforce terms not brought to the licensee's attention or terms that would cause most licensees to refuse the license if the term was brought to their attention. *Id.* However, the proposed law will not require that the licensee actually review the terms of the mass-marketed license. *Id.*

411. The vast majority of attorneys representing both licensors and licensees favor the enforceability of shrink-wrap agreements. Slightly more attorneys representing vendors approved of shrink-wrap agreements. The qualitative portion of the study revealed strong support for procedural protection for mass-marketed shrink-wrap. Many of the respondents questioned the general enforceability of shrink-wrap unless customers were given an opportunity to read and agree to the terms. CLA Survey, Fall 1994 (see *infra* App. B question 5).

412. CLA Survey, Fall 1994 (on file with author).

413. See Lemley, *supra* note 408, at 1252 (discussing cases in which shrink-wrap licenses were found to be "contracts of adhesion" because the consumer lacked a "meaningful choice as to the terms offered").

Article 2B may not dispose of all controversy surrounding the shrink-wrap agreement.⁴¹⁴ However, its balancing of procedural protection with the enforceability of standard form agreements may help to avoid the stalemate between licensors and licensees which has characterized the debate over shrink-wrap licenses.

8. CONCLUSION

In spite of the continuing mass-market license controversy, Article 2B as a whole will make great strides in elucidating the legal landscape of software licensing. For instance, by treating computer software as a license rather than as a good, Article 2B will mold commercial law to fit Internet security software. The proposed Article will also likely clarify the key issues regarding the transfer of security software that are not dealt with in Article 2 and provide much-needed certainty for the developers and constituents of the National Information Infrastructure. Although there is at present only minimal Internet or network case law, it is likely that much future litigation involving Internet security software will revolve around performance standards, warranties and damages. Indeed, the lack of case law is one of the strongest arguments for adopting the proposed Article 2B to provide a uniform starting point to resolve these issues.

B. The Case for Adopting the Proposed Article 2B for Internet Security Software

Lon Fuller wrote that "judges and writers on legal topics frequently make statements they know to be false. These statements are called 'fictions'." ⁴¹⁵ Fuller compared the use of legal "fictions" to a children's game of imagination triggered by "let's play."⁴¹⁶ For the

414. For example, Mark Lemley advocates additional limitations on shrink-wrap licensing. He proposes that the drafters revise Proposed U.C.C. § 2-2203 by augmenting the draft with the following language:

(b) The terms adopted under subsection (a) include all of the terms of the mass-market license without regard to the individual knowledge or understanding of the licensee. However, a term does not become part of the license if the term:

...

(4) creates an obligation or imposes a limitation on the licensee that is inconsistent with federal intellectual property law, or that deprives the licensee of a right or privilege granted the licensee under federal intellectual property law.

Lemley, *supra* note 408, at 1292.

415. LON L. FULLER, *LEGAL FICTIONS* 1 (1967).

416. *Id.*

past decade, courts have pretended that U.C.C. Article 2 applies to the licensing of software. As early as 1988, the court in *Communication Groups, Inc. v. Warner Communications* stated that "it seems clear that computer software, generally, is considered by the courts to be a tangible . . . item."⁴¹⁷ As we have seen, however, software is not tangible. Aside from the physical diskette, software is an intangible collection of magnetically-fixed electronic impulses. Judges are employing a legal fiction when they assume that software is a tangible. Jeremy Bentham would attack this stretching of sales law as a manifestation of the "pestilential breath of Fiction."⁴¹⁸

A "white lie" is also necessary to stretch sales law to the licensing of Internet security products.⁴¹⁹ The vast majority of these products consist entirely or primarily of computer software. They are licensed in a property transfer transaction which is wholly different from sales in both character and result. Von Ihering argued that "[f]ictions are makeshifts, crutches to which science ought not to resort."⁴²⁰

Applying Article 2 to computer software has been a useful fiction. Even Von Ihering acknowledged it is "better that science should go on crutches than to slip without them, or not to venture to move at all."⁴²¹ Nevertheless, the time has come for the courts and Internet security industry to dispense with fictions, white lies and crutches. Article 2B will provide an adequate legal infrastructure for structuring Internet security product transactions. Article 2B will place the law of licensing in accord with commercial and technological realities, clarify ownership dilemmas, approximate more closely international commercial law's tender and performance standards, and accommodate virtually all licensing of intangibles transactions, even continuous-access contracts.

1. CONVERGENCE WITH COMMERCIAL AND TECHNOLOGICAL REALITY

The proposed Article 2B will comport well with commercial practices already existing in the Internet security industry. Licensors

417. *Communication Groups, Inc. v. Warner Communications*, 138 Misc. 2d 80, 83 (N.Y. Civ. Ct. 1988).

418. FULLER, *supra* note 412, at 2 (citing JEREMY BENTHAM, WORKS (1843)).

419. *Id.* at 5 (quoting Von Ihering who called fictions the "white lies" of the law. VON IHERING, GEIST DES ROEMISCHEN RECHTS AUF DEN VERSHIEDENEN STUFEN SEINER ENTWICKLUNG (6th ed. 1924) (The title of this book translates as "The Spirit of Roman Law in the Various Stages of its Development."))

420. *Id.* at 2 (quoting Von Ihering).

421. *Id.*

already negotiate software licensing agreements under the aegis of U.C.C. concepts.⁴²² Contract is the law-in-action being used in marketing Internet security software. For example, licensors grant, limit or disclaim warranties using the prescribed methodology of the U.C.C.⁴²³ Remedies and default terms are negotiated in accordance with U.C.C. principles. A period of acceptance testing is typically built into customized transactions.⁴²⁴ The performance standards of Internet security products are assessed against the benchmark of U.C.C. norms such as good faith, fair dealing and usages of trade. Since mid-century, the U.C.C. has gained hegemony as an influential source of contract law.⁴²⁵ The proposed Article 2B will thus codify commercial practice norms that are already widely accepted.

Article 2B will also adapt U.C.C. standards to the technological realities of Internet security contracting. Given the virtual impossibility of delivering software which contains no errant lines of code, Article 2's perfect tender rule will be replaced by a substantial performance standard. In addition, Article 2's concept of the physical "delivery" of tangibles—which does not fit with the transfer of limited rights in intangible software—will be replaced in the proposed Article 2B with the notion of transfer of rights. The transfer of rights provision will be flexible enough to accommodate transfers of intangibles which occur across electronic media, by remote access or through methods not yet conceived. Moreover, under the proposed Article 2B, the automatic passing of title currently found in Article 2 will be superseded by the provision that the *parties' agreement* will determine the scope of any property rights conveyed in a license transaction. Article 2B will thus eliminate the danger that common law judges could presume that title passes with a license; it will grant licensors default protection not presently assured under common law.⁴²⁶

Furthermore, the proposed Article 2B will address obligations especially applicable to the licensing of Internet security products. These include maintenance and support obligations of the licensor, and

422. See, e.g., *Colonial Life Ins. Co. v. Electronic Data Systems Corp.*, 817 F. Supp. 235, 238-39 (D. N.H. 1993); *Advent Sys. Ltd. v. Unisys Corp.*, 925 F.2d 670, 673-76 (3rd Cir. 1991); *Schroders, Inc. v. Hogan Systems, Inc.*, 137 Misc. 2d 738, 741-42 (N.Y. 1987) (applying warranty law to computer networks). See also *infra* App. A §§ 14-15, 17.

423. See, e.g., *infra* App. A § 14.

424. *Id.*

425. See ALAN SCHWARTZ, *COMMERCIAL TRANSACTIONS: PRINCIPLES AND POLICIES* 2 (1982).

426. Cf. *Sheets v. Yamaha Motors Corp.*, 849 F.2d 179 (5th Cir. 1988) (stating that trade secret protection may be lost by permitting third parties to have access to confidential information).

nondisclosure and confidentiality obligations of both the licensor and licensee. For example, Article 2B will validate a norm of confidentiality for protecting intellectual property commodities.⁴²⁷ Confidentiality is the *sine qua non* of Internet security products.⁴²⁸ The proposed software article would presume that a licensee is not entitled to underlying data or code unless the parties expressly agree to the contrary.⁴²⁹ Furthermore, no assignment may be made that would endanger another party's confidential material.⁴³⁰ A licensee will also not be permitted to resell or transfer materials in its possession after a rightful rejection.⁴³¹ Confidentiality of data and data protection will be so strongly embedded in the new licensing provisions as to survive even dissolution of the contract.⁴³²

Professor Nimmer noted that: "Many intangibles contracts deal with information the value of which is linked to the maintenance of secrecy or confidentiality about the information or technology it describes."⁴³³ Fifty percent of the CLA Survey respondents favored the imposition of a confidentiality obligation on the end-user with respect to non-public information obtained from mass-marketed software.⁴³⁴ The proposed Article 2B will thus recognize and address the well-established concern of confidentiality with respect to the licensing of intangibles such as Internet security products.

2. INTERNATIONALIZATION OF THE INTERNET

Another reason for adoption and use of Article 2B is the growing internationalization of commercial law. The United States is now subject to the United Nations' Convention on Contracts for the International Sale of Goods (CISG).⁴³⁵ If the countries of both parties are signatories to the CISG, then the CISG applies by default and not

427. See, e.g., U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

428. See, e.g., *infra* App. A § 13(c)(ii).

429. See, e.g., U.C.C. § 2-2206 (Proposed Draft, Feb. 10, 1995).

430. See, e.g., U.C.C. § 2-2502 (Proposed Draft, Feb. 10, 1995).

431. See, e.g., U.C.C. § 2-2307 (Proposed Draft, Feb. 10, 1995).

432. See, e.g., U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

433. U.C.C., Rev. Article 2, Sales, Chapter 3: Licenses, Prefatory Note 10 (Proposed Draft Sept. 10, 1994) (Raymond Nimmer, Reporter).

434. CLA Survey, Fall 1994 (*see infra* App. B question 7).

435. The Convention on Contracts for the International Sale of Goods applies to sales of goods between parties whose places of business are in different states that have signed the Convention. See Convention on Contracts for the International Sale of Goods, 1988, Art. 1 (1), reprinted in COMMERCIAL AND DEBTOR-CREDITOR LAW at 1642 (Douglas G. Baird et al. eds., 1994).

the U.C.C.⁴³⁶ Thus, as more security software is marketed across borders, it is important that American law harmonize with international commercial law. Unfortunately, there are dramatic differences between the U.C.C. and the CISG.⁴³⁷ For example, the CISG does not follow the perfect tender rule of U.C.C. section 2-601. Instead, the CISG has adopted a fundamental breach standard for breach of an obligation, such that a buyer may receive substitute goods only if the delivered goods fundamentally breach the sales contract.⁴³⁸ In contrast, Article 2 permits a buyer to obtain substitute goods if the goods fail "in any respect to conform to the contract."⁴³⁹ These two standards are clearly incompatible.

The proposed Article 2B, on the other hand, is likely to be strikingly similar to the CISG. For example, the proposed Article's concept of substantial performance will likely be functionally equivalent to the CISG's fundamental breach standard. The CISG's definition of "fundamental breach" is: some unexcused failure of performance which "substantially deprives" a party of an entitlement under the contract.⁴⁴⁰ This definition is essentially the "substantial performance" standard of the proposed Article 2B.⁴⁴¹ Therefore, the

436. *Id.* Since the United States is a signatory, CISG applies in any sales transactions with parties of another signatory state. However, Art. 6 of CISG permits the parties to opt out of CISG ("the parties may exclude the application of this Convention"). *Id.* at 1643. The parties may decide to apply the U.C.C. or the proposed Article 2B. In the former case, they may select the law which will govern their rights and duties provided that, in choosing which state's codification applies, they select a jurisdiction which bears a "reasonable relation" to their transaction. U.C.C. § 1-105(1) (1990). In the latter case, the parties will likely be able to select any state's law so long as it does not "contradict fundamental public policy of a more related state." U.C.C. § 2-109(a) (Proposed Draft, Feb. 10, 1995).

437. See generally JOHN HONNOLD, UNIFORM LAW FOR INTERNATIONAL SALES UNDER THE 1980 UNITED NATIONS CONVENTION (2d ed. 1991).

438. Article 25 of the Convention on the International Sale of Goods (CISG) states: A breach of contract committed by one of the parties is fundamental if it results in such detriment to the other party as substantially to deprive him of what he is entitled to expect under the contract, unless the party in breach did not foresee and a reasonable person of the same kind in the same circumstances would not have foreseen such a result.

Convention Relating to a Uniform Law on the International Sale of Goods, July 1, 1964, 834 U.N.T.S. 107, art. 25.

439. See U.C.C. §§ 2-691, 2-711, 2-712 (1990).

440. See generally C.M. BIANCA & M.J. BONELL, COMMENTARY ON THE INTERNATIONAL SALES LAW—THE 1980 VIENNA SALES CONVENTION 205 (1987); JOHN HONNOLD, UNIFORM LAW FOR INTERNATIONAL SALES (1982).

441. See, e.g., U.C.C. § 2-2306 (Proposed Draft, Feb. 10, 1995). Technically, the proposed "hub and spoke" version still allowed jurisdictions to choose either the extant perfect tender rule corresponding to U.C.C. § 2-601 or the substantial performance standard. U.C.C. § 2-2403(b) (Proposed Draft, Feb. 10, 1995). Due to its

juristic truth is that there will be a closer fit between the proposed Article 2B and the norms of the CISG than between Article 2 and CISG. Therefore, adoption of the proposed Article will be one large step closer to harmonization of American and international commercial software law.

The CISG, however, does not explicitly address software licensing. Like Article 2, the CISG is designed for tangible goods and can only apply to the licensing of intangibles by analogy. Further, the CISG does not address problems of contract formation. Essentially, the CISG is a barrier to creating a uniform international body of law for the licensing of intangibles just as Article 2 is a barrier to creating a uniform American software licensing law.

A uniform commercial law of the Internet that applies no matter where the parties reside must be formulated. It should remove barriers to trade and facilitate commercial transactions across the Internet. Although uniform proposals for software protection have been put forth in recent years as part of the General Agreement on Tariffs and Trade (GATT) and in the Council of the European Communities Directive on the Protection of Computer Programs, they are limited in scope.⁴⁴² The ideal solution would be to formulate a new Convention for Software Licensing on the Internet that would provide uniform rules governing transnational Internet contracts, and would be tailored to take into account radically different social, economic and legal systems. The proposed Article 2B might be considered as a possible model since it will provide the vocabulary and the concepts for dealing with intangibles.

3. FLEXIBILITY AND DETERMINACY IN THE LAW

The principal argument for adopting the proposed Article 2B will be its flexibility. Mark Lemley notes that "technological development in the computer industry has outrun the pace of legal

impracticability, however, the perfect tender option is not expected to remain in the final version of Article 2B.

442. See General Agreement on Tariffs and Trade—Multilateral Trade Negotiations (The Uruguay Round): Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Part II, § 1 (Dec. 15, 1993). GATT has limited application because agreements under GATT apply only between governments. *Id.* at Part I. The Council of the European Communities Directive on the Protection of Computer Programs is limited because it applies only to "computer programs" and "preparatory design work" leading to computer programs. *Preamble*, The Council of the European Communities Directive on the Protection of Computer Programs, 1991 O.J. (L 122) 42.

change."⁴⁴³ The proposed Article will offer resolution to this problem. In addition, the accommodation of commercial law to Internet and network security software has the potential of providing comprehensive coverage of licensing to other intangibles and intellectual property as well.

The proposed Article 2B will likely encompass "intangibles contracts and agreements incidental to intangible contracts, including agreements to support, maintain or modify software."⁴⁴⁴ Internet security transactions are often a mixture of sales, licenses and services. These transactions will be treated under the proposed Article, with the exception of the sales aspects of such transactions, which will continue to be treated under Article 2. The scope of the proposed Article, however, will conceivably cover all information licensing contracts.

For example, the proposed software article's reach will likely be broad enough to encompass even continuous access contracts⁴⁴⁵ such as those for the services of CompuServe, Prodigy, America Online, WESTLAW and LEXIS.⁴⁴⁶ Security software will be increasingly marketed to provide privacy and confidentiality when using on-line services. Article 2B will establish specialized default rules tailored for those services, and for other continuous-access contracts.⁴⁴⁷ Most notably, access availability and resolution of disputes with regard to OSPs will be set by usage of trade.⁴⁴⁸ Thus, the proposed software licensing article's recognition of trade usage as a standard is consistent with the U.C.C.'s goal of codifying accepted business practices.⁴⁴⁹

443. Mark A. Lemley, *Convergence in the Law of Software Copyright?*, 10 HIGH TECH. L.J. 1,3 (1995).

444. U.C.C. § 2-2102 (Proposed Draft, Feb. 10, 1995).

445. *See id.*

446. The proposed Article 2B will likely define a "continuous access contract" as a: contract that transfers a right or privilege to have access over a period of time to an intangible, resource, data system, or other facility under the control of the licensor or a third party, and gives the transferee a right of access at a time substantially of its own choosing subject to limitations on the general availability of the intangible, resource, data system or other facility.

U.C.C. § 2-102(13) (Proposed Draft, Feb. 10, 1995).

447. One of the norms will be that access "be available at times and in a manner consistent with . . . express commitments in the contract," or consistent with industry standards. U.C.C. § 2-2314(a) (Proposed Draft, Feb. 10, 1995).

448. For example, neither isolated failures nor scheduled downtime for maintenance will place the OSP licensor in breach. *See, e.g.*, U.C.C. §§ 2-2314 (b), (c) (Proposed Draft, Feb. 10, 1995).

449. One of the key concepts of the U.C.C. is the use of prevailing industry customs to shape contract interpretation and remedies. *See* U.C.C. § 1-205(2) (1994).

There is a widespread feeling in the industry that the law of software contracting is indeterminate. In the CLA Survey, respondents emphasized the need for certainty and clarification of the law of intangibles. Article 2B will address these concerns. The proposed Article's capacity to advance, accommodate and protect changing technologies is precisely why it will be the appropriate template for intangibles. Adoption of the proposed Article for licensing of intangibles will reduce the uncertainty of litigating the potential applicability of an Article 2 provision that is at odds with the more delimited transfer of intellectual property rights. Although not perfect, the proposed Article 2B provides a model of default rules and gap-fillers for parties to either adopt or draft around. It will go a long way toward simplifying, clarifying and modernizing the law governing Internet security products and all licensing of intangibles.

The exact terms of Article 2B are still in flux. The drafters recognize that, in order for software law reform to be effective, they must engineer consensus among diverse stakeholders, such as software industry representatives, U.C.C. stakeholders and consumers. They also must balance the interests of licensors, licensees, consumers, third parties and the public. The drafters are attempting to ensure that these numerous interests and issues will be addressed. For example, care has been taken to establish clear ground rules for a three-party relationship that arises in the intangibles contracting context. The objective is to balance the goals of contract law with the provision of appropriate incentives to minimize the risk of injury.

The proposed Article 2B is an entirely new paradigm that has been specifically drafted for licensing. It substitutes commercial and technological realities for legal fictions. The proposed software licensing article provides a comprehensive, yet flexible, framework upon which all the parties—licensors and licensees, vendors and vendees, merchants, and consumers—may build and structure their Internet security transactions.

V. CONCLUSION

Law does not descend disembodied from the thin, rarefied air of the legal heavens.⁴⁵⁰ The Law of Cyberspace must be forged and molded. It should rely on traditional legal theories only insofar as it produces outcomes which maximize society's benefit in the long run. The legal infrastructure for intangibles must "accommodate itself to

450. Felix S. Cohen, *Transcendental Nonsense and The Functional Approach*, 35 COLUM. L. REV. 809, 809 (1935) (coining the term of the legal heavens "reserved for the theoreticians of the law").

the changing thought and action."⁴⁵¹ During its formative period, especially, the infrastructure must be given some room to develop.⁴⁵²

Like the builders of nineteenth century canals and railroads who benefited from legal doctrines such as the fellow servant rule, contributory negligence and assumption of risk, the builders of the National Information Infrastructure (NII) should be free to contract and allocate liability among themselves and their users. Article 2B affords this freedom of contract to licensors of Internet security products and other intangibles within accepted parameters of good faith and conscionability. The NII is just beginning to emerge. If the NII is saddled with too much tort or statutory liability, its development may be endangered.

Experience rather than logic must guide commercial law.⁴⁵³ The Uniform Commercial Code has been the most successful codification experience in American history. Modernizing the U.C.C. to accommodate Internet security products and intangibles will best facilitate the development of the NII. The proposed Article 2B will accomplish this goal.

451. FOWLER V. HARPER & FLEMING JAMES, JR., *THE LAW OF TORTS* xxvii (1956) (arguing that the law of torts has historically proven to be very adaptable).

452. LAWRENCE M. FRIEDMAN, *A HISTORY OF AMERICAN LAW* 409-27 (1973).

453. Justice Oliver Wendell Holmes' famous aphorism was that the life of the law is experience not logic: "The law embodies the story of a nation's development through many centuries In order to know what it is, we must know what it has been, and what it tends to become." OLIVER W. HOLMES, *THE COMMON LAW* 1 (1881).

APPENDIX A

EXAMPLE OF SALES AND LICENSE AGREEMENT OF A
NETWORK SECURITY PRODUCT

Appendix A provides an example of sales and license agreement for a information security product. This agreement also employs many U.C.C. concepts and methods. For example, there are provisions for warranties, disclaimers, limitations, modification and "sole and exclusive" remedies.

Agreement No.:

COMPANY X
AGREEMENT FOR PURCHASE OF EQUIPMENT
AND LICENSE OF SOFTWARE

This Agreement is made this _____ day of _____, 19____ by and between COMPANY X, a Delaware corporation with its principal place of business at _____ ("XXX"), and the Customer, its affiliates and subsidiaries whose name and address are set forth below (the "Customer").

Name of Customer:

Bill To:

Ship To (if different):

Street

Street

City

City

State Zip Code

State Zip Code

Telephone Number: ()

Telephone Number: ()

Point of Contact:

Point of Contact:

The Customer agrees to purchase and XXX, by its acceptance and execution of this Agreement, agrees to sell and/or license, on the terms and conditions set forth in the Terms and Conditions of Sale and Software License Agreement attached hereto, the equipment, software, firmware and features listed below (the "Products").

Customer:

Company X:

Name

Name

Signed

Signed

Title

Title

TERMS AND CONDITIONS
OF SALE AND
SOFTWARE LICENSE AGREEMENT

The Products sold and/or licensed under this Agreement consist of hardware, software and firmware. Unless otherwise expressly provided in this Agreement, all sales or licenses of Products by XXX are made in accordance with and subject to the following terms and conditions, except that to the extent that the Products constitute software and/or firmware, they are not sold to the Customer but are licensed to the Customer under Section 13 of this Agreement.

1. **Prices.** The Customer may rely only on prices published by XXX or quoted in writing from an authorized XXX representative, which prices may be changed at any time without notice. Written quotations expire automatically thirty (30) calendar days from the date issued and are subject to change or termination by notice during that period. All prices are subject to adjustment on account of specifications, quantities, shipment arrangements or other terms and conditions which are not part of the original price quotation. The purchase prices, license fees and other charges for the Products shall be as set forth in this Agreement or, if no prices have been specified, shall be XXX's established prices in effect at the time of shipment. Unless otherwise expressly stated in writing, all prices are F.O.B. XXX's facility in Cambridge, Massachusetts.

2. **Taxes.** Prices are exclusive of all federal, state, municipal or other excise, sales, use, occupational or similar taxes now in force or enacted in the future, all of which shall be paid by the Customer, except for such taxes as are imposed on XXX's income. XXX may invoice the Customer for any such taxes and remit any payments made on any such invoice directly to the appropriate taxing authorities. The Customer is responsible for obtaining and providing to XXX any certificate of exemption or similar document required to exempt any sale or license from sales, use or similar tax liability.

3. **Terms of Payment.** Unless otherwise expressly stated in writing, payment terms for the Products (together with any invoiced charges for shipping, insurance and applicable taxes) are net thirty (30) days from date of invoice. XXX reserves the right at any time to require full or partial payment in advance, or to revoke any credit previously extended, if, in XXX's judgment, the Customer's financial condition does not warrant proceeding on the terms specified. Overdue payments shall be subject to finance charges computed at a periodic rate (to the extent permitted by law) of 1 1/2% per month (18% per year), plus all costs and expenses, including reasonable attorney's fees, incurred by XXX in collecting such overdue amounts.

4. **Delivery.** The requested delivery date for each of the Products is stated on the second page of this Agreement. XXX will use reasonable efforts to meet requested delivery dates, but does not represent or warrant that it will, in fact, meet such dates, all shipments being subject to XXX's availability schedule. Shipping dates are also based upon prompt receipt of all necessary information from the Customer. XXX shall not be liable for any delay in delivery, or failure to deliver, due to causes beyond its control, including, without limitation, acts of nature, acts or omissions of the Customer, acts of civil or military authority, fires, lockouts, strikes and slowdowns, floods, epidemics, quarantine restrictions, wars, riots, delays in transportation, unavailability of supplies or sources of energy, or delays in delivery by XXX's suppliers. In the event of delay due to any such cause, the time for delivery shall be extended for a period equal to the duration of the delay, and the Customer shall not be entitled to refuse delivery or otherwise be relieved of any obligation as a result of the delay.

5. **Shipment.** Unless specific instructions to the contrary are set forth in this Agreement, XXX will select methods and routes of shipment. XXX will not assume any liability in connection with shipment or constitute any carrier as its agent. All shipments will be insured at the Customer's expense and made at the Customer's risk, and the Customer shall be responsible for making claims with carriers, insurers, warehousemen and others for misdelivery, non-delivery, loss, damage or delay. All transportation, rigging, draying and handling charges, and all insurance costs, shall be paid by the Customer. XXX may, at its option, invoice the Customer for any such charges and remit any payments directly to the shipper and/or insurer.

6. **Title and Risk of Loss.** Subject to the terms set forth in Section 7 below and to XXX's right to stop delivery of Products in transit, title to and risk of loss for Products shall pass to the Customer upon the earlier of delivery (a) to the Customer or (b) to a carrier for shipment to the Customer; provided, however, that title to the Software and User Documentation (as such terms are defined in Section 13 of this Agreement) shall at all times remain with XXX.

7. **Security Interest.** As security for the payment and performance by the Customer of all of its liabilities and obligations under this Agreement, the Customer hereby grants to XXX a security interest in the Products (together with their products and proceeds, including all credit, fire or other insurance proceeds). The Customer acknowledges that a copy of this Agreement may be filed with the appropriate authorities as a financing statement in order to evidence the security interest granted to XXX. In addition, the Customer agrees to execute and deliver such financing statements and other documents as XXX requests to perfect the security interest granted hereby.

8. Cancellations.

(a) Cancellation of Standard Orders. Except as set forth in paragraph (b) below, the Customer may cancel any order for Products under this Agreement at any time before shipment without the payment of any cancellation charge. If any order is canceled by the Customer after shipment of the Products, then (i) the Customer shall pay the cost of shipment to the Customer's site and the cost of returning any such Products to XXX, (ii) risk of loss shall remain with the Customer until such Products have been returned to XXX, and (iii) the Customer shall pay an administrative fee of \$150 to XXX for each such canceled order.

(b) Cancellation of Non-Standard Orders. In the event that the Customer cancels a non-standard order at any time prior to shipment, then the Customer agrees to pay the full price of any (i) custom applications, as described on the second page of this Agreement, and (ii) completed components, sub-assemblies and/or finished assemblies (which may include full production runs) of non-standard Products (i.e., Products fabricated to meet the Customer's requirements, drawings, specifications or other designs). No cancellations shall be permitted after non-standard Products have been shipped.

9. Installation. Unless otherwise specified in this Agreement, the Customer assumes sole responsibility for the installation of Products at the Customer's premises.

10. Specifications. All products are subject to XXX's standard tolerances for specifications. XXX reserves the right to make substitutions and modifications in the specifications of any Products; provided, that such substitutions or modifications do not materially adversely affect the performance of the Products or the purposes for which they can be used.

11. Use of Data. Any specifications, drawings, technical information or other data furnished by XXX to the Customer shall remain the property of XXX, shall be kept confidential by the Customer, and shall be returned to XXX promptly upon XXX's request.

12. Claims for Non-Conforming Shipments. All claims for non-conforming shipments must be made in writing to XXX within ten (10) days of delivery of goods to the Customer. Any claims not made within that period shall be deemed waived and released.

13. Software License.

(a) Definitions. For purposes of this Agreement:

(i) "Host System" shall mean the hardware and other computer equipment in connection with which the Products are utilized, as set forth on the second page of this Agreement.

(ii) "User Documentation" shall mean the manuals, handbooks and other written materials relating to the Software and the Products provided by XXX to the Customer.

(iii) "Software" shall mean all software and firmware, including all computer programs, whether in the form of tape, disk, ROM or other memory storage, incorporated in or used in connection with the Products and provided by XXX to the Customer, consisting of a series of instructions or statements in machine-readable, object code form only, and all modifications, refinements and improvements thereto made by XXX which XXX provides to the Customer.

(b) Grants of License. XXX hereby grants, and the Customer hereby accepts, a royalty-free, non-exclusive, nontransferable license, without the right to sublicense, subject to the terms and conditions of this Agreement, to use the Software on and in connection with the Host System and to utilize the User Documentation, for the Customer's internal purposes only. No right or license is granted under this Agreement for the use or other utilization of the Software, directly or indirectly, for the benefit of any other person or entity or in conjunction with any equipment other than the Host System.

(c) Ownership, Intellectual Property Rights and Non-Disclosure.

(i) Title to and ownership of the Software, including patents, copyrights and property rights applicable thereto, shall at all times remain solely and exclusively with XXX, and the Customer shall not take any action inconsistent with such title and ownership.

(ii) The Customer shall not cause or permit disclosure, copying, display, loan, publication, transfer of possession (whether by sale, exchange, gift, operation of law, or otherwise) or other dissemination of the Software or User Documentation, in whole or in part, to any third party without the prior written consent of XXX. The Customer shall take all reasonable steps to safeguard the Software and User Documentation and to ensure that no unauthorized persons have access to the Software and User Documentation, and that no persons authorized to have such access shall take any action which would be prohibited by this Agreement if taken by the Customer. The Customer shall promptly report to XXX any actual or suspected violation of this clause (ii) and shall take such further steps as may reasonably be requested by XXX to prevent or remedy any such violation.

(iii) The Customer shall include and shall not alter or remove any copyright, trade secret, proprietary and/or other legal notices contained on or in the Products, Software and User Documentation. The existence of any such copyright notice on the Products, Software or User Documentation shall not be construed as an admission, or deemed to create a presumption, that publication of such material has occurred.

(iv) The Customer shall promptly respond to all reasonable inquiries by XXX concerning the Customer's compliance with the provisions of this paragraph (c) of this Section 13.

(d) Acknowledgment of No Program Rights. The Customer acknowledges that XXX is the owner of the Software and the User Documentation for purposes of Section 117 of the Copyright Act of 1976, as amended, and for all other purposes, and that XXX intends that the Customer will use the Software and the User Documentation only in accordance with the terms and conditions of this Agreement. Physical copies of the Software and the User Documentation shall be deemed to be on loan to the Customer during the term of the license granted hereunder.

(e) Modification of Software. The Customer shall not modify, enhance or otherwise change or supplement the Software without the prior written consent of XXX.

(f) Term of License. XXX may terminate the license of the Software granted hereunder, by written notice to the Customer, if the Customer fails to comply with any of the terms or conditions of this Agreement. Within ten (10) days after any termination of this license hereunder, the Customer shall destroy or return to XXX the original and all copies (including partial copies) of the Software and the User Documentation and shall certify in writing to XXX that it has done so. The Customer shall pay any shipping and handling charges necessary to return the Software and the User Documentation to XXX. Any further obligations of the parties shall cease upon termination of this Agreement; provided, that the terms and conditions of Sections 11, 15, 16 and 18 and paragraph (c) of this Section 13 shall continue in full force and effect for a period of five (5) years following the termination of this Agreement.

14. Warranty.

(a) Equipment.

(i) XXX warrants that the Products (to the extent not constituting Software) shall in all material respects be free from defects in material and workmanship for a period of ninety (90) days from the date of shipment. Any claims of defects not made within such 90-day period shall be deemed waived and released.

XXX's sole obligation with respect to claims of defects made within the warranty period described above shall be, at its option, to repair or replace any item which it determines to be defective, either at XXX's facility or the Customer's facility, at the discretion of XXX. All transportation charges to such facility will be prepaid by the Customer, and XXX will pay all return transportation charges. XXX may employ used parts to make repairs or replacements, so long as the used parts are not defective in any respect and are of a quality equivalent to new parts. All replaced parts will become the property of XXX on an exchange basis.

(ii) All Card Modules are guaranteed, unless subjected to unreasonable use or physical abuse, for the purchased life set forth on the second page of this Agreement, to functionally perform in conformity with XXX product literature in all material respects, including physical integrity, battery life, functional integrity, and synchronization with the Products so long as XXX implementation requirements are maintained for use on the Host System.

(b) Software. During the first ninety (90) days following shipment of the Software, XXX will, upon receipt of a problem report from the Customer, correct all documented code errors determined by XXX to be such and caused by a defect in an unaltered version of the Software delivered to the Customer. Any claims of nonconformance which are not made within such 90-day period shall be deemed waived and released. XXX's sole obligation with respect to claims of nonconformance shall be to remedy the nonconformance (either by repair or replacement, at XXX's option) when reported to it by the Customer. This warranty shall not apply (i) if the Software has been modified or altered by the Customer and (ii) in the event that repair or replacement cannot be made or is ineffective due to the operational characteristics of any Host System.

(c) Limitations of Warranty. The foregoing warranty shall not apply if (i) repair or replacement is required as a result of causes other than normal use, including, without limitation, repair, maintenance, alteration or modification of the Products by persons other than XXX or other XXX-authorized personnel, accident, fault or negligence of the Customer, operator error or improper use or misuse of the Products, or causes external to the Products such as, but not limited to, failure of electrical power or fire or water damage; or (ii) the Products are modified by the Customer or used with software or equipment other than the Host System. The Customer acknowledges and accepts responsibility for his or its selection of the Products to achieve the Customer's intended results, for his or its use of the Products and for the results obtained thereby. The Customer also accepts responsibility for the selection and use of, and the results obtained from, any other equipment, software or services used in conjunction with the Products. XXX's liability for damages to the Customer for any cause, regardless of the form of action, shall not exceed the aggregate price paid for the Products under this Agreement.

(d) No action, whether in contract or tort, including negligence, arising out of or in connection with this Agreement, may be brought by either party more than two years after the cause of action has accrued. This paragraph (d) shall not apply to actions for any breach of the provisions of Section 17 or actions by XXX for violations or infringements of XXX's rights relating to the Software licensed hereunder.

OTHER THAN AS SET FORTH IN THIS SECTION 14, XXX DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE PRODUCTS (INCLUDING, WITHOUT LIMITATION, WARRANTIES AS TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE), EITHER EXPRESS OR IMPLIED, AND THE FOREGOING EXPRESS WARRANTIES ARE IN LIEU OF ALL LIABILITIES OR OBLIGATIONS ON THE PART OF XXX. IN NO EVENT WILL XXX BE LIABLE FOR LOSS OF USE, DATA OR PROFITS, OR OTHER SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF ANY PRODUCTS, EVEN IF XXX HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

15. **Limitation of Liability.** The express obligations contained in this Agreement are in lieu of all liabilities or obligations of XXX for damages, including, but not limited to, general, special or consequential damages arising out of or in connection with the delivery, use or performance of the Products, Software and/or User Documentation, or arising from the negligence of XXX, its employees, officers, directors, or consultants. In addition, the Customer further agrees that:

(a) In no event will XXX be liable to the Customer for lost profits or similar damages or for any claims against the Customer by any other party; and

(b) XXX's liability to the Customer for damages resulting from any cause whatsoever shall be limited to the charges paid by the Customer for use of the Products, Software and/or User Documentation, as the case may be, relating to the cause of such damages.

16. **Documentation.** All documentation with respect to the Products, including, without limitation, training documentation, software documentation and maintenance manuals and drawings, is furnished solely for the Customer's internal use. The Customer may make copies of such documentation to satisfy its internal requirements, provided that all such copies include copyright and proprietary information notices. No other copies or use of such documentation, or any portion thereof, shall be made without the prior written approval of XXX.

17. **Patent and Copyright Indemnity.** If notified promptly in writing of any action (and provided that XXX has been promptly notified of all prior claims relating to such action) brought against the Customer based on a claim that the

current, unaltered release of the Products, Software or User Documentation supplied to the Customer infringes a United States patent or copyright, XXX shall defend such action at its expense and pay any costs or damages finally awarded in such action which are attributable to such claim, provided that XXX shall have sole control of the defense of any such action and all negotiations for its settlement or compromise. If a final injunction is obtained against the Customer's use of any of the Products, Software or User Documentation by reason of infringement of a United States patent or copyright, or if in XXX's opinion any of the Products, Software or User Documentation supplied to the Customer hereunder is likely to become the subject of a successful claim of infringement of a United States patent or copyright, XXX shall, at its option and expense, either procure for the Customer the right to continue using such Products, Software or User Documentation, as the case may be, or replace or modify the same so that it becomes non-infringing, or grant the Customer a credit for such Products, Software or User Documentation, as the case may be, and accept its return. Notwithstanding the foregoing, XXX shall not have any liability to the Customer under this Section 17 if the infringement or claim is based upon (i) the use of any of the Products, Software or User Documentation in combination with other equipment or software which is not furnished by XXX, (ii) Products, Software or Product Documentation which have been modified or altered by the Customer, or (iii) the furnishing to the Customer of any information, service or application assistance. The Customer shall indemnify and hold XXX harmless against any expense, judgment or loss for infringement of any patents, copyrights or trademarks as a result of XXX's compliance with the Customer's designs, specifications or instructions. No cost or expenses shall be incurred for the account of XXX without the prior written consent of XXX. IN NO EVENT SHALL XXX'S TOTAL LIABILITY TO THE CUSTOMER UNDER THIS SECTION 17 EXCEED THE AGGREGATE SUM PAID TO XXX BY THE CUSTOMER FOR THE ALLEGEDLY INFRINGING EQUIPMENT OR PROGRAM. THE FOREGOING STATES THE ENTIRE LIABILITY OF XXX WITH RESPECT TO INFRINGEMENT OF PATENTS OR COPYRIGHTS BY ANY OF THE PRODUCTS, SOFTWARE OR USER DOCUMENTATION OR ANY PART THEREOF OR THEIR OPERATION.

18. Injunctive Relief. Because unauthorized use or transfer of the Software or User Documentation, or any information contained therein, may diminish substantially the value of such materials and may irrevocably harm XXX, if the Customer breaches the provisions of Sections 11 or 16 or paragraph (c) of Section 13 of this Agreement, XXX shall (without limiting its other rights or remedies) be entitled to equitable relief (including but not limited to injunctive relief) to protect its interests and, if the Customer has not returned the Software and the User Documentation to XXX, or certified to XXX's satisfaction that the Software and the User Documentation have been destroyed, XXX shall have the right to enter and take possession of the Software and the User Documentation wherever located without liability for damage, so long as XXX shall have acted reasonably and in good faith.

19. Notices. All notices given by either party to the other party under this Agreement shall be in writing and personally delivered or sent by registered or certified mail, return receipt requested, to the other party at its address set forth above. The date of personal delivery or the date of mailing, as the case may be, shall be deemed to be the date on which such notice is given.

20. General.

(a) The obligations of XXX under this Agreement shall be subject to the procurement by, and at the expense of, the Customer of any import or export licenses, documents, permits or clearances required with respect to this Agreement and are subject to the condition precedent that all necessary approvals from governmental authorities have been obtained. The Customer agrees at all times to comply with all laws of the United States of America and its 50 states applicable to the Customer and shall not take, or refrain from taking, any action which would result in the violation of such laws by XXX. Nothing contained in this Agreement shall be construed as creating a joint venture, partnership or employment relationship between the parties.

(b) The validity, construction and interpretation of this Agreement and the rights and duties of the parties hereto shall be governed by and construed in accordance with the laws of The Commonwealth of Massachusetts.

(c) This Agreement constitutes the entire understanding between the Customer and XXX with respect to the subject matter hereof, and XXX makes no representations to the Customer except as expressly set forth herein.

(d) Terms and conditions set forth in any purchase order or other document provided by the Customer to XXX which differ from, conflict with or are not included in this Agreement shall not be part of any agreement between XXX and the Customer unless specifically accepted by XXX in writing. To the extent that this document may constitute an acceptance, such acceptance is expressly conditioned on the Customer's assent to any additional or inconsistent terms and conditions set forth in this document.

(e) This Agreement shall not be deemed or construed to be modified, amended or waived, in whole or in part, except by written agreement of the parties hereto.

(f) The Customer may not assign this Agreement, or any of its rights or obligations hereunder, without the prior written consent of XXX.

(g) Section headings are for descriptive purposes only and shall not control or alter the meaning of this Agreement.

(h) All rights and remedies of either party shall be cumulative and may be exercised singularly or concurrently. The failure of either party, in any one or more instances, to enforce any of the terms of this Agreement shall not be construed as a waiver of future enforcement of that or any other term.

(i) If any provision of this Agreement shall for any reason be held illegal or unenforceable, such provision shall be deemed separable from the remaining provisions of this Agreement and shall in no way affect or impair the validity or enforceability of the remaining provisions of this Agreement.

(j) XXX shall not be liable for failure to fulfill any of its obligations under this Agreement due to causes beyond its control.

SCHEDULE OF PRODUCTS

1. Description of Products

Qty	Model	Description	Price
-----	-------	-------------	-------

3. Total Purchase

Price:	\$
--------	----

Taxes:	\$
--------	----

Shipping:	\$
-----------	----

TOTAL:	\$
--------	----

(due net thirty days from date of invoice)

4. Requested Delivery Date:

5. Host System:

Manufacturer

Model

Serial No.

Operating System

Location

APPENDIX B

COMPUTER LAW ASSOCIATION SURVEY AND RESULTS

This survey was mailed to all 950 members of The Computer Law Association in August of 1995. The membership consists of intellectual property attorneys who develop, distribute and use computer technology. We received 147 responses to the survey which represented a 15% response rate. For more information regarding the survey and respondents, see note 305.

Reproduced below is the text of the survey questions and the answers from which the respondents could choose. The bracketed numbers represent the total number of respondents (not the percentage) who selected that particular answer. Neither the space provided for commentary nor the actual comments are reproduced here. All comments made by respondents are on file with co-author Michael Rustad.

Survey results were compiled by Elaine Martel.

I. GENERAL INFORMATION ABOUT RESPONDENT

A. Which category best describes your background?

(Check the single, most appropriate, box)

Consumer, not a business	[0]
Software	[44]
High tech electronics (hardware)	[16]
Chemicals	[1]
Legal services	[69]
Financial services	[1]
Consumer products	[1]
Government/public	[2]
Academic	[2]
Medical distributor	[1]
Utility	[0]
Service industry	[8]
Other (please identify)	[0]

B. The size of your 1992 sales were approximately:

\$1 million to under \$10 million	[21]
\$10 million to under \$100 million	[25]
\$100 million to under \$1 billion	[17]
Over \$1 billion	[17]

C. Your business involvement with software is primarily as a:

(Check All Boxes Appropriate)

Purchaser/licensee of software	[70]
Seller/licensor of software owned by your company	[55]
Reseller of software	[18]
Consultant	[84]
Software developer	[38]
Service bureau	[8]

D. You work primarily with:

(Check All Boxes Appropriate)

Custom developed or customized software	[109]
Industry specific software	[104]
Mass marketed software	[87]
Horizontal system software	[7]
Other (please identify)	[0]

E. Your function primarily is:

(Check All Boxes Appropriate)

Sales	[0]
Purchasing	[0]
Information systems	[0]
Software developer	[0]
Consumer	[0]
Legal	[all]
Other (please identify)	[0]

F. Personal info:

(Check All Boxes Appropriate)

Male	[127]
Female	[20]
Attorney	[all]
Sales	[0]
Other	[0]
Under 5 years involvement with software	[70]
5—15 years involvement with software	[95]
Over 15 years involvement with software	[45]

G. In your software transactions, what type of agreements do you often use?

(Check All Boxes Appropriate)

Signed license agreement or development agreement	[132]
Unsigned "shrink wrap" license	[91]
Purchase order	[58]
Electronic license (without written agreement)	[24]
No formal agreement	[17]
Detailed contracts supplementing license terms	[97]
Other (please identify)	[0]

H. For which types of agreements do you frequently obtain legal review of software agreements before signing?

(Check All Boxes Appropriate)

Signed license agreement or development agreement	[103]
Unsigned "shrink wrap" license	[31]
Purchase order	[23]
Electronic license (without written agreement)	[14]
No formal agreement	[7]
Detailed contracts supplementing license terms	[76]
Other (please identify)	[0]

II. SUBSTANTIVE QUESTIONS

1. DEFINITION

Mass marketed software should be defined:

	Agree	No Opinion	Disagree
Based on number of copies licensed to date	[42]	[20]	[66]
Based on method of distribution	[104]	[11]	[16]
Based on the type of end user	[57]	[24]	[42]
Based on form of license agreement (e.g., license agreements that did not provide for signatures by the parties would automatically qualify)	[72]	[17]	[39]
Based on price	[28]	[25]	[72]

2. ASSIGNABILITY

Regardless of any shrink wrap license restrictions, the law should allow the end user to:

	Agree	No Opinion	Disagree
Assign or resell software	[83]	[11]	[49]
Move the physical location of software	[122]	[2]	[19]
Use software forever	[73]	[16]	[52]
Resell rightfully rejected software to recover costs	[45]	[23]	[70]
Assign software to an outsourcing vendor (a company hired to manage data processing activities; software may need to be moved, run at a different location, etc.)	[79]	[15]	[46]

3. WARRANTY

The following warranties should be included with all shrink wrap software and MAY NOT BE DISCLAIMED:

	Agree	No Opinion	Disagree
The software vendor has the right to license the software product	[127]	[5]	[13]
The software vendor has no knowledge of infringement of any third party rights	[105]	[13]	[27]
The software product does not infringe any third party proprietary rights	[69]	[22]	[53]
The software product will operate substantially in accordance with its accompanying user documentation	[110]	[10]	[24]
The software product contains no expiration dates or disabling routines	[58]	[27]	[58]
The software product contains no viruses, worms [or] other malicious routines	[74]	[34]	[43]
The software product contains no routines to prevent unauthorized use	[22]	[35]	[85]

4. WARRANTY

The following warranties should be included with all shrink wrap software UNLESS CONSPICUOUSLY DISCLAIMED by the seller:

	Agree	No Opinion	Disagree
The software vendor has the right to license the software product	[63]	[11]	[55]
The software vendor has no knowledge of infringement of any third party rights	[56]	[18]	[54]
The software product does not infringe any third party proprietary rights	[46]	[20]	[64]
The software product will operate substantially in accordance with its accompanying user documentation	[75]	[8]	[46]
The software product contains no expiration dates or disabling routines	[64]	[17]	[54]
The software product contains no viruses, worms [or] other malicious routines	[50]	[19]	[64]
The software product contains no routines to prevent unauthorized use	[54]	[20]	[61]

5. SCOPE OF RIGHTS GRANTED*The law should provide that:*

	Agree	No Opinion	Disagree
Shrink wrap licenses are enforceable contracts	[85]	[14]	[45]

6. SCOPE OF RIGHTS GRANTED*Regardless of any shrink wrap license provisions, the end user should have the right to:*

	Agree	No Opinion	Disagree
Load and execute the software on a single computer	[141]	[0]	[5]
Make back-up copies	[138]	[2]	[5]
Reverse engineer the software to determine & exploit underlying non-copyrightable ideas	[52]	[18]	[76]
Load software on a network file server and make it available to a single user at a time	[91]	[15]	[38]
Load software on a network file server and make available to an unlimited number of users	[5]	[19]	[120]
Load software on a network and make available to users for a usage fee	[33]	[21]	[90]

7. SCOPE OF RIGHTS GRANTED*Regardless of any shrink wrap provisions, shrink wrap software should:*

	Agree	No Opinion	Disagree
Impose an obligation of confidentiality on the end user with respect to non-public information obtained from the software	[61]	[22]	[60]

In the following hypothetical situations please respond based on your view of what the applicable law should be.

8. HYPOTHETICAL

A consumer purchases shrink-wrap software, uses the software for one year, then sells the software and documentation. The consumer does not maintain a copy of the software after it is sold.

Statement—Regardless of any shrink-wrap license restrictions against the “rental, resale, or transfer,” a buyer should have the right to resell the shrink-wrap software.

For	Against	No Opinion
[97]	[43]	[6]

9. HYPOTHETICAL

Detailed shrink wrap license conditions state that the software may not be “rented, sold or transferred”.

Statement—The purchaser should be able to install this software on a computer, even if this computer is rented to patrons for \$10.00 per hour.

For	Against	No Opinion
[47]	[82]	[16]

10. HYPOTHETICAL

A consumer purchases entertainment software. The software is shrink wrap software and contains a variety of disabling routines designed to permit use of the software only until Dec. 31, 1994. The company also sells a perpetual license of the same product at a higher cost.

Statement—If the software is conspicuously labeled, the seller should be able to include disabling routines and enforce shrink wrap license restrictions designed to grant non-perpetual software license.

For	Against	No Opinion
[120]	[18]	[7]

11. HYPOTHETICAL

A consumer buys a new furnace which contains software designed to control furnace performance. The software contains disabling routines which render the furnace inoperable unless the consumer pays an annual maintenance fee for service and updates to the software. This restriction is clearly labeled on the furnace and spelled out in shrink-wrap license restrictions.

Statement—By conspicuous labeling, a seller should be able to include disabling routines and enforce non-perpetual license restrictions for software embedded in, or designed to work with, other products.

For	Against	No Opinion
[61]	[75]	[9]

12. HYPOTHETICAL

A business purchases this furnace in order to develop alternate software by reverse engineering the furnace and the software. New software is developed which does not violate any patents or copyrights.

Statement—Regardless of any shrink-wrap license restrictions included with the furnace prohibiting “reverse engineering, decompiling, or disassembly of the software”, the business should be able to license use of this newly developed software.

For	Against	No Opinion
[80]	[49]	[16]

13. SOFTWARE “SPOKE” OF THE PROPOSED UCC

Have you heard about the newly proposed software “spoke” for Article Two of the UCC?

Yes	No
[58]	[86]

ARTICLE

LENDING THE FEDERAL CIRCUIT A HAND: AN ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS

TIMOTHY J. DOUROS †

TABLE OF CONTENTS

I.	INTRODUCTION	322
II.	PROVISIONS AND PURPOSES OF THE PATENT ACT.....	324
	A. Constitutional and Statutory Basis.....	324
	B. Goals of the American Patent System.....	325
III.	INFRINGEMENT AND THE DOCTRINE OF EQUIVALENTS	326
	A. Infringement Generally.....	326
	B. Infringement Under the Doctrine of Equivalents	327
IV.	ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS	330
	A. The Hand Formula	331
	B. Transformation of the Hand Formula: The Economic Doctrine of Equivalents	332
	C. Criticisms and Strengths of the Economic Doctrine of Equivalents.....	345
V.	APPLICATION OF THE ECONOMIC DOCTRINE OF EQUIVALENTS	348
	A. Application Generally	348
	B. Application to <i>Graver Tank</i>	350
VI.	CONCLUSION	352

© 1995 Timothy J. Douros.

† Associate, Morgan & Finnegan, L.L.P., New York; J.D., 1995, Boston College; A.B., 1990, Dartmouth College.

I. INTRODUCTION

The Court of Appeals for the Federal Circuit was created,¹ in part, to bring uniformity to judicial rulings in the area of patent law.² Nowhere in the patent law is such uniformity more needed than in application of the doctrine of equivalents.³ Since the Supreme Court gave the doctrine modern acceptance in *Graver Tank & Manufacturing Co. v. Linde Air Products Co.*,⁴ application of the doctrine has been a source of controversy for courts,⁵ scholars,⁶ and practitioners.⁷

In *Graver Tank*, the Supreme Court held that where an accused device does not literally infringe the claims of the patentee's device, infringement may be found under the doctrine of equivalents, if the accused device performs *substantially* (1) the same function (2) in the

1. The U.S. Constitution, Article III, § 1, provides for the creation of "such inferior Courts as the Congress may from time to time ordain and establish."

2. Federal Courts Improvement Act of 1982, Pub. L. No. 97-164, 96 Stat. 25; *see also* S. REP. NO. 275, 97th Cong., 2d Sess. 11 (1982), *reprinted in* 1982 U.S.C.C.A.N. 11, 11 (stating that the statute is "part of a comprehensive program designed to improve the quality of our Federal court system.") The Act withdrew the jurisdiction of the twelve regional Courts of Appeals.

3. The veracity of this statement is partially due to the Federal Circuit's efficacy in clarifying other areas of the patent law. *See generally* Rochelle Cooper Dreyfuss, *The Federal Circuit: A Case Study in Specialized Courts*, 64 N.Y.U. L. REV. 1 (1989); Douglas A. Strawbridge et al., *Patent Law Developments in the United States Court of Appeals for the Federal Circuit During 1986*, 36 AM. U. L. REV. 861 (1987).

4. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605 (1950).

5. *See, e.g.*, *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1545 (Fed. Cir. 1995) (en banc) (Plager, J., dissenting) (stating that the majority failed "to bring a consistent and rationalized practice to the doctrine of equivalents"); *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 939 (Fed. Cir. 1987) (en banc) (Bennett, J., dissenting) (accusing the majority of "contraven[ing] Supreme Court precedents . . . [and] rewrit[ing] the doctrine of equivalents without regard for stare decisis principles"); *Graver Tank*, 339 U.S. at 613 (Black, J., dissenting) (stating that the majority opinion "steriliz[es] . . . Acts of Congress and prior decisions").

6. *See, e.g.*, Martin J. Adelman & Gary L. Francione, *The Doctrine of Equivalents in Patent Law: Questions that Pennwalt Did Not Answer*, 137 U. PA. L. REV. 673, 728-29 (1989) (arguing that justice would best be served if the doctrine of equivalents were abandoned); Timothy L. Tilton, *The Doctrine of Equivalents in Patent Cases*, 32 J. PAT. OFF. SOC'Y 861 (1950) (predicting that the Supreme Court would use *Graver Tank* to abolish the doctrine of equivalents).

7. *See, e.g.*, Rudolph P. Hofmann, Jr., *The Doctrine of Equivalents: Twelve Years of Federal Circuit Precedent Still Leaves Practitioners Wondering*, 20 WM. MITCHELL L. REV. 1033, 1060 (1994) ("uncertainty remains in every issue of the doctrine of equivalents as currently applied"). Tom Arnold, of Arnold, White & Durkee, observed that different panels of the Federal Circuit "have gone off on frolics of their own in an effort to render the doctrine narrower and more specific. And they have generated one hell of a turmoil, with opinions that don't reconcile with each other." Victoria Slind-Flor, *Rethinking Protection: Software Patents, Copyright Issues Shaped the IP Landscape in '93*, NAT'L L.J., Jan. 24, 1994, at S27.

same way (3) to achieve the same result.⁸ Judge Plager described judicial frustration with the doctrine of equivalents thusly:

[One] problem with the doctrine is that appellate review of many of these doctrine of equivalents cases is largely pro forma. Federal district judges, perhaps understandably, by and large make little pretense of liking these patent infringement cases, and are quite content to give them, and all the issues in them, to juries to decide. The cases typically come to us on appeal with nothing more than a general verdict finding infringement. There is no explanation by the jury of the rationale behind their verdict, if any exists.⁹

Recently, the Federal Circuit restated the test for infringement under the doctrine of equivalents.¹⁰ In *Hilton Davis*, the court sought to enunciate a formulation of the doctrine of equivalents that is both consistent with the tripartite test described in *Graver Tank* and amenable to proper application by trial courts. Specifically, the Federal Circuit held that "application of the doctrine of equivalents rests on the substantiality of the differences between the claimed and accused products or processes, assessed according to an objective standard."¹¹ Thus, the standard for equivalency is insubstantial difference between the accused device and the patent claim.¹² Further, the court held that the function/way/result test of *Graver Tank* is but one method of demonstrating insubstantial difference.¹³ In addition, the majority resisted the temptation to delimit application of the doctrine of equivalents by, for example, rendering it an equitable remedy¹⁴ or requiring an element of intent.¹⁵ Finally, the *Hilton Davis* court, by stating that "the doctrine of equivalents provides the same protection to the substance of the claim scope provided by the doctrine of literal infringement,"¹⁶ has reaffirmed the proposition that "[a]pplication of the doctrine of equivalents is the exception, . . . not the rule, for if the public comes to believe (or fear) that the language of patent claims can never be relied on, . . . then claims will cease to serve their intended purpose."¹⁷

8. 339 U.S. at 608-09.

9. *Hilton Davis*, 62 F.3d at 1538 (Plager, J., dissenting).

10. *Id.* at 1516.

11. *Id.* at 1518.

12. *Id.*

13. *Id.*

14. *Id.* at 1521.

15. *Id.* at 1519.

16. *Id.* at 1528.

17. *London v. Carson Pirie Scott & Co.*, 946 F.2d 1534, 1538 (Fed. Cir. 1991).

This article describes an economic equation, modeled after the Hand Formula,¹⁸ that addresses both the goals of the Patent Act and the purpose of the doctrine of equivalents. In addition to addressing these concerns, the equation, which is referred to in this article as the Economic Doctrine of Equivalents, removes some of the subjectivity of the traditional doctrine of equivalents and provides for greater ease of judicial application. The equation may be used for two different, but related, purposes. First, it may be used to analyze and explain judicial interpretation of the doctrine of equivalents from an economic perspective. Second, the equation serves as a guide to future judicial application of the doctrine of equivalents by providing judges with a framework for evaluating the most important considerations of the doctrine of equivalents and a method for applying those considerations to a particular case.

Part II of this paper examines the Patent Act and its purposes, in order to elucidate the underlying policies and concerns of patent protection. Part III examines infringement in general, and the doctrine of equivalents in particular, in light of the policy goals of the Patent Act. Part IV describes the elements of the Economic Doctrine of Equivalents. Part V discusses the application of the Economic Doctrine of Equivalents and applies it to the facts of *Graver Tank* to demonstrate the consistency of the economic formulation with the aims of the traditional analysis under the doctrine of equivalents. Part VI is the conclusion.

II. PROVISIONS AND PURPOSES OF THE PATENT ACT

Any consideration of the doctrine of equivalents must begin with an examination of the patent system generally. Moreover, proper application of any interpretation of the doctrine of equivalents requires an understanding of the purposes of the Patent Act.¹⁹ In this way, courts, attorneys and scholars may avoid a construction of the doctrine of equivalents that is inconsistent with the Patent Act.

A. Constitutional and Statutory Basis

The Constitution of the United States grants Congress the power "[t]o promote the . . . useful Arts, by securing for limited Times to . . . Inventors the exclusive Right to their . . . Discoveries."²⁰ This

18. *United States v. Carroll Towing*, 159 F.2d 169 (2d Cir. 1947).

19. The current patent statute is 35 U.S.C. §§ 1-376 (1988).

20. U.S. CONST. art. I, § 8, cl. 8.

constitutional provision gave rise to the first Patent Act in 1790.²¹ While the Patent Act has been revised numerous times since the first act, the patent system has remained substantially the same since 1836.

B. Goals of the American Patent System

In the broadest sense, the American patent system is designed to provide an economic incentive for technological advancement and investment in scientific research.²² Furthermore, by requiring full disclosure of the subject matter to be patented, the system provides for dissemination of information that is critical to further technological advances. The patent system encourages both invention and investment, and presumes that consequential benefits, in the form of wealth and information, will accrue to society.²³ The patent is an economic reward which allows the inventor to exclude others from manufacturing, using, or selling the invention for a limited period of time. Given the widespread antipathy toward monopolies²⁴ that existed at the time the Constitution was drafted, the Founding Fathers must have had a strong belief that the patent system, though potentially harmful, would result in an overall benefit to society.²⁵

21. An Act to promote the progress of useful Arts, ch. 7, 1 Stat. 109 (1790) (repealed 1793).

22. See, e.g., Robert P. Merges & Richard R. Nelson, *On the Complex Economics of Patent Scope*, 90 COLUM. L. REV. 839 (1990) (detailing the economic benefits that result from the patent system).

23. But see FRIEDRICH A. VON HAYEK, *THE FATAL CONCEIT: THE ERRORS OF SOCIALISM* (1989); Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity*, 61 AM. ECON. REV. 561 (1971).

24. A patent, of course, is not a monopoly. As then-Chief Judge Markey observed, "[i]t is but an obfuscation to refer to a patent as 'the patent monopoly' or to describe a patent as an exception to the general rule against monopolies." *Schenck, A.G. v. Norton Corp.*, 713 F.2d 782, 786 n.3 (Fed. Cir. 1983). However, given the development of the patent law from the English law of monopolies, the tradition of mischaracterizing a patent as a monopoly is understandable. The Case of Monopolies, *Darcy v. Allin*, 77 Eng. Rep. 1260 (K.B. 1602), was the first English case to declare a royal patent grant void as contrary to the common law and in violation of many acts of Parliament. Later, in *The Clothworkers of Ipswich*, *Godbolt*, 252, 78 Eng. Rep. 147 (K.B. 1615), the court recognized that while the Crown did not have power to grant a monopoly in a specific trade, it could grant an exclusive right for a limited time to an inventor who introduced a new discovery. Later, in 1623, Parliament enacted the Statute of Monopolies, 21 Jam. ch. 3, which served both to codify the common law and provide a statutory basis for the British patent law. See generally Edward C. Walterscheid, *The Early Evolution of the United States Patent Law: Antecedents* (pts. 1 & 2), 76 J. PAT. & TRADEMARK OFF. SOC'Y 697, 849 (1994).

25. Thomas Jefferson, an inventor and member of the commission created by the 1790 Patent Act to oversee the patent system, observed that only those "things which are worth to the public the embarrassment of an exclusive patent" deserve patent

The modern view of the patent system, backed by substantial economic analysis,²⁶ is not qualitatively different from the views held by the drafters of the Constitution. The basic notion that the patent system provides an incentive to invent and invest, outweighing the dangers of monopoly, is still the prevailing view.²⁷ Much recent criticism of the patent system focuses on the inefficient allocation of resources to "block" alternative patentable methods in order to preserve the value of one's patent.²⁸ Because these efforts contribute nothing substantial to society's technological understanding or aggregate wealth, patent protection is unwarranted. Therefore, the patent system ideal is to provide incentives for invention and investment in areas that will be useful to society, while minimizing the effects of inefficient allocation of resources that result from duplicative, insubstantial research.

III. INFRINGEMENT AND THE DOCTRINE OF EQUIVALENTS

A. Infringement Generally

The Patent Act provides that "whoever without authority makes, uses or sells any patented invention, within the United States during the term of the patent therefor, infringes the patent."²⁹ In determining whether an accused device³⁰ infringes a patent, either

protection. *Graham v. John Deere Co.*, 383 U.S. 1, 10-11 (1966). James Madison concluded that the public good resulting from a patent grant coincided with the inventor's right to the invention and that the individual states could not effectively regulate the matter. THE FEDERALIST NO. 43, at 288 (James Madison) (Jacob E. Cooke ed., 1961).

26. See, e.g., Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977); WILLIAM D. NORDHAUS, *INVENTION, GROWTH, AND WELFARE: A THEORETICAL TREATMENT OF TECHNOLOGICAL CHANGE* (1969); Yoram Barzel, *Optimal Timing of Innovations*, 50 REV. ECON. & STAT. 348 (1968); John S. McGee, *Patent Exploitation: Some Economic and Legal Problems*, 9 J.L. & ECON. 135 (1966); F.M. SCHERER ET AL., *PATENTS AND THE CORPORATION* (2d ed. 1959); Arnold Plant, *The Economic Theory Concerning Patents for Inventions*, 1 *ECONOMICA* 30 (1934).

27. For an excellent discussion of intellectual property generally and government incentives to technological progress, see Edmund W. Kitch, *Property Rights in Inventions, Writings and Marks*, 13 HARV. J.L. & PUB. POL'Y 119 (1990).

28. See, e.g., SUBCOMMITTEE ON PATENTS, TRADEMARKS AND COPYRIGHTS, SENATE COMM. ON THE JUDICIARY, 85TH CONG., 2D SESS., AN ECONOMIC REVIEW OF THE PATENT SYSTEM 15 (Comm. Print 1958) (Fritz Machlup).

29. 35 U.S.C. § 271(a) (1988).

30. As used in this article, the word "device" means any patentable subject matter under 35 U.S.C. § 101 (1988).

literally or under the doctrine of equivalents, a court must ascertain the meaning and limits of the patentee's claims and then apply those claims to the accused device.³¹ This determination is made for both literal infringement and infringement under the doctrine of equivalents.³² Literal infringement occurs when an accused device incorporates all of the claims of the patented device.³³

B. Infringement Under the Doctrine of Equivalents

1. THEORETICAL BASIS OF THE DOCTRINE OF EQUIVALENTS

The doctrine of equivalents is a judicial construction which recognizes the frailties of the written word.³⁴ Because, as one scholar has noted, "[a]n infringer appropriates an invention, not words,"³⁵ infringement may occur even though the accused device does not directly infringe upon the literal words of the patentee's claims. To deny recovery for infringement by a device that does not literally infringe upon the claims of a patent, but which nonetheless imitates the patented device, "would be to convert the protection of the patent grant into a hollow and useless thing."³⁶ A court may consider infringement under the doctrine of equivalents only after it has determined that there is no literal infringement.³⁷

31. *Key Mfg. Group, Inc. v. Microdot, Inc.*, 925 F.2d 1444, 1448 (Fed. Cir. 1991); *Palumbo v. Don-Joy*, 762 F.2d 969, 974 (Fed. Cir. 1985); *Texas Instruments, Inc. v. United States Int'l Trade Comm'n*, 805 F.2d 1558, 1568-70 (Fed. Cir. 1986) [hereinafter *Texas Instruments I*].

32. *Texas Instruments I*, 805 F.2d at 1568-70; *SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985); *Martin v. Barber*, 755 F.2d 1564, 1567 (Fed. Cir. 1985).

33. *Laitram Corp. v. Rexnord, Inc.*, 939 F.2d 1533, 1535 (Fed. Cir. 1991); *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1580 (Fed. Cir. 1989); *Julien v. Zeringue*, 864 F.2d 1569, 1571 (Fed. Cir. 1989).

34. *See Winans v. Denmead*, 56 U.S. (15 How.) 330, 343 (1853) (observing that "where the whole substance of the invention may be copied in a different form, it is the duty of courts and juries to look through the form for the substance of the invention"); *Zeigler v. Philips Petroleum Co.*, 483 F.2d 858 (5th Cir.), *cert. denied*, 414 U.S. 1079 (1973) (recognizing the doctrine of equivalents as a safeguard against the elevation of form over substance); *cf. Cabell v. Markham*, 148 F.2d 737, 739 (2d Cir. 1945) (Judge Hand noting that "it is one of the surest indexes of a mature and developed jurisprudence not to make a fortress out of the dictionary"). *But cf. White v. Dunbar*, 119 U.S. 47, 51 (1886) (warning that a patent claim is not "like a nose of wax which may be turned and twisted in any direction").

35. 1A LESTER HORWITZ, *PATENT OFFICE RULES AND PRACTICE* § 111.6 (1992).

36. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 607 (1950).

37. *Id.* at 607-08. However, there is no equitable threshold for application of the doctrine of equivalents. "The doctrine of equivalents has no equitable or subjective

2. APPLICATION OF THE DOCTRINE OF EQUIVALENTS

In *Graver Tank*, the Supreme Court established a tripartite test for infringement under the doctrine of equivalents by stating that the doctrine is predicated on the theory that "if two devices do the same work in substantially the same way, and accomplish substantially the same result, they are the same, even though they differ in name, form, or shape."³⁸ The *Graver Tank* Court considered two electric welding compositions.³⁹ The patented composition was a combination of alkaline earth metal silicate and calcium fluoride.⁴⁰ The accused composition used silicates that were not of an alkaline earth metal.⁴¹ In all other respects, the compositions were identical.⁴² The Court relied on the prior art to establish that persons skilled in the art would have understood that the accused composition could be substituted for (i.e., was equivalent to) the claimed composition.⁴³ Therefore, the doctrine of equivalents was applied to prevent the accused device from fraudulently circumventing the patent.⁴⁴ The rationale behind the doctrine, the Court said, is that "one may not practice a fraud on a patent."⁴⁵ Simply put, the doctrine prevents a person from circumventing a patent by use of an equivalent means, if that means would have been obvious to one skilled in the art of the patent.

The method for determining equivalency to a claim or limitation of the patented device varies depending on the facts of a specific case.⁴⁶ Some cases hold that the focus must be on the combination as a whole,⁴⁷ while others indicate that an equivalent of every claim limitation must be found in the accused device.⁴⁸ In either case, the

component." *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1523 (Fed. Cir. 1995) (en banc).

38. *Graver Tank*, 339 U.S. at 608 (quoting *Machine Co. v. Murphy*, 97 U.S. 120, 125 (1877)).

39. *Graver Tank*, 339 U.S. at 610.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.* at 611-12.

44. *Id.* at 612.

45. *Id.* at 608.

46. *Malta v. Schulmerich Carillons, Inc.*, 952 F.2d 1320, 1326 (Fed. Cir. 1991) ("How equivalency . . . is met necessarily varies from case to case due to many variables such as the form of the claim, the nature of the invention defined by it, the kind of limitation that is not literally met, etc.").

47. *Texas Instruments I*, 805 F.2d 1558, 1568-70 (Fed. Cir. 1986).

48. *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 934-36 (Fed. Cir. 1987) (en banc).

appropriate comparison is between the accused device and the patent claim, not simply a comparison of the two devices.⁴⁹

3. PIONEER INVENTIONS

In the case of a pioneer invention,⁵⁰ the patented device is entitled to broad protection under the doctrine of equivalents.⁵¹ This broad protection arises from the dearth of relevant prior art, rather than an expansive interpretation of the patent claims.⁵² Conversely, a patented device that constitutes only a slight improvement in an area of substantial prior art will receive limited protection against infringement under the doctrine.⁵³

4. RESTRICTIONS ON THE DOCTRINE OF EQUIVALENTS

The two major restrictions on the doctrine of equivalents are "prosecution history estoppel"⁵⁴ and limits imposed by the prior art.⁵⁵ Under prosecution history estoppel, a patentee is estopped from asserting infringement of claims which are embodied in the accused device but were rejected during prosecution of the patentee's patent.⁵⁶ The purpose of this doctrine is to prevent the patentee from benefiting from claims that were clearly rejected by the Patent Office and are not within the scope of the patent.⁵⁷ The range of equivalents to

49. *Read Corp. v. Portec, Inc.*, 970 F.2d 816, 822 n.2 (Fed. Cir. 1992). The court provided the example of the comparison between a pencil and a pen: while the two "may for many purposes or uses be generally equivalent, . . . claim limitations drawn to a pen would not under the doctrine of equivalents cover a pencil and vice versa." *Id.*

50. The Supreme Court defined a pioneer invention as "a wholly novel device, or one of such novelty and importance as to mark a distinct step in the progress of the art, as distinguished from a mere improvement or perfection of what had gone before." *Westinghouse v. Boyden Power Brake Co.*, 170 U.S. 537, 562 (1898). More simply, a pioneer invention is an invention without significant prior art. *Texas Instruments I*, 805 F.2d at 1572.

51. *Morley Sewing-Mach. Co. v. Lancaster*, 129 U.S. 263, 272-84 (1889); *Perkin-Elmer Corp. v. Westinghouse Elec. Corp.*, 822 F.2d 1528, 1532 (Fed. Cir. 1987) (citing *Sealed Air Corp. v. United States Int'l Trade Comm'n*, 645 F.2d 976, 984 (C.C.P.A. 1981)).

52. *Texas Instruments v. United States Int'l Trade Comm'n*, 846 F.2d 1369, 1370 (Fed. Cir. 1988).

53. *Hughes Aircraft Co. v. United States*, 717 F.2d 1351, 1362 (Fed. Cir. 1983).

54. This is alternatively known as file wrapper estoppel. *Amstar Corp. v. Envirotech Corp.*, 730 F.2d 1476, 1485 (Fed. Cir. 1984).

55. *Stewart-Warner Corp. v. City of Pontiac, Mich.*, 767 F.2d 1563, 1572 (Fed. Cir. 1985).

56. *Schriber-Schroth Co. v. Cleveland Trust Co.*, 311 U.S. 211, 220-21 (1940); *Black & Decker, Inc. v. Hoover Serv. Ctr.*, 866 F.2d 1285, 1295 (Fed. Cir. 1989).

57. *Mannesmann Demag Corp. v. Engineered Metal Prods. Co.*, 793 F.2d 1279, 1284 (Fed. Cir. 1986).

which a claimed invention is entitled is also limited in that it may not include what was prior art when the patent was prosecuted.⁵⁸

A further restriction on the doctrine of equivalents is the "reverse doctrine of equivalents." As the *Graver Tank* Court noted, if "a device is so far changed in principle from a patented article that it performs the same or similar function in a substantially different way, but nevertheless falls within the literal words of the claim, the doctrine of equivalents may be used to restrict the claim and defeat the patentee's action for infringement."⁵⁹ Thus, where an invention relies on the fundamental concept embodied in a patent but is more sophisticated than the patented device due to "a significant advance," the accused device does not infringe by virtue of the reverse doctrine of equivalents.⁶⁰ Once a patentee establishes literal infringement, the burden is on the alleged infringer to establish noninfringement under the reverse doctrine of equivalents.⁶¹

The symmetry of the doctrine of equivalents and the reverse doctrine of equivalents extends to their faults as well. That is, if it is difficult to determine whether a device is not substantially different from a patented device such that there is infringement, it will not be much easier to determine whether a device that falls within the literal words of the claim is so substantially different that infringement does not occur.

IV. ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS

Patent infringement may be thought of as a federal law tort.⁶² Although this analogy is inapposite in some circumstances,⁶³ similarities between patent infringement and tort law render the

58. *Stewart-Warner*, 767 F.2d at 1572.

59. *Graver Tank*, 339 U.S. at 608-09.

60. *Mead Digital Sys., Inc. v. A.B. Dick Co.*, 723 F.2d 455, 464 (6th Cir. 1983).

61. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1123-24 (Fed. Cir. 1985).

62. *See, e.g., Beverly Hills Fan Co. v. Royal Sovereign Corp.*, 21 F.3d 1558, 1570-71 (Fed. Cir. 1994) (for purposes of a state's long-arm statute, the situs of the tort of patent infringement is not the domicile of the patentee but the place where the allegedly infringing activity takes place); *A.C. Aukerman Co. v. R.L. Chaides Constr. Co.*, 960 F.2d 1020, 1031 (Fed. Cir. 1992) (laches is an appropriate defense to continuing torts, such as patent infringement); *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1579 (Fed. Cir. 1986) (infringement is a tort for purposes of corporate liability); *Carbice Corp. v. Am. Patents Dev. Corp.*, 283 U.S. 27, 33 (1931) ("[i]nfringement, whether direct or contributory, is essentially a tort").

63. *See, e.g., North Am. Philips Corp. v. Am. Vending Sales, Inc.*, 35 F.3d 1576, 1579 (Fed. Cir. 1994) ("[W]hile it may be appropriate to speak loosely of patent infringement as a tort, more accurately the cause of action for patent infringement is created and defined by statute.").

former amenable to analysis incorporated in the latter. The level of *mens rea* required, the remedies available and the general economic impact all facilitate infringement analysis by traditional tort law methods.⁶⁴ Therefore, the following analysis and transformation of tort law principles, guided by patent law purposes, is a logical extension of economic analysis into the realm of the patent law.

A. The Hand Formula

In 1947, Judge Learned Hand first posited a framework for an economic interpretation of negligence. In *United States v. Carroll Towing*,⁶⁵ Judge Hand recognized the economic considerations involved in determining whether a party has acted reasonably.⁶⁶ A person's duty to protect against injuries resulting from his behavior is determined by relating: (1) the probability that the injury will occur; (2) the magnitude of the resulting injury; and (3) the burden of taking precautions to prevent the injury from occurring.⁶⁷ Judge Hand asserted that liability for injury resulting from certain action attaches when the burden (B) is less than the product of the probability (P) and the magnitude of the injury (L).⁶⁸ This relationship is summarized in a simple algebraic formula as $B < P \cdot L$.⁶⁹ When the burden of preventing the accident is greater than the product of the probability and magnitude of the injury ($B > P \cdot L$), the actor has not acted negligently and arguably should not be liable for any injury resulting from his actions.

The rationale for this approach is that tort law should encourage economically desirable behavior.⁷⁰ As Judge Posner observed:

When the cost of accidents is less than the cost of prevention, a rational profit-maximizing enterprise will pay tort judgments to the accident victims rather than incur the larger cost of avoiding liability. Furthermore, overall economic value or welfare would

64. See generally RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* (4th ed. 1992); WERNER Z. HIRSCH, *LAW AND ECONOMICS* (2d ed. 1988).

65. 159 F.2d 169 (2d Cir. 1947).

66. See generally Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 32 (1972).

67. *Carroll Towing*, 159 F.2d at 173.

68. *Id.*

69. While the formula may be simple, the conceptual and practical application may not be. Judge Hand himself recognized the problems that may arise in applying the test: "The difficulties are in applying the rule, . . . they arise from the necessity of applying a quantitative test to an incommensurable subject matter; and the same difficulties inhere in the concept of 'ordinary' negligence." *Moisan v. Loftus*, 178 F.2d 148, 149 (2d Cir. 1949).

70. Posner, *supra* note 66, at 32-33.

be diminished rather than increased by incurring a higher accident-prevention cost in order to avoid a lower accident cost. If, on the other hand, the benefits in accident avoidance exceed the costs of prevention, society is better off if those costs are incurred and the accident is averted, and so in this case the enterprise is made liable, in the expectation that self-interest will lead it to adopt the precautions in order to avoid a greater cost in tort judgments.⁷¹

Thus, by this view, tort law should not deter activity by attaching liability where the cost of preventing any resulting injury exceeds the cost of the injury itself. In this way, the law promotes economic efficiency.

B. Transformation of the Hand Formula: The Economic Doctrine of Equivalents

By considering the purposes of the patent law in general, and of the doctrine of equivalents in particular, it is possible to design an equation similar in nature to the Hand Formula that may be used to determine infringement under the doctrine of equivalents. Commercial viability, in conjunction with investment and obviousness considerations, may be used directly in considering infringement under the doctrine of equivalents.⁷² These concepts may be related in an equation to facilitate application of the doctrine of equivalents. According to the formulation, an accused device does not infringe under the doctrine of equivalents when its obviousness (O), as measured by investment (reflected in the prior art) in the problem addressed by the accused device,⁷³ is less than the product of direct investment (I) in the accused device⁷⁴ and the commercial viability (C_v) of the accused device, defined as the increased efficiency, measured in dollars, created by the accused device.⁷⁵ Thus, where $O < C_v \cdot I$, there is no infringement under the doctrine of equivalents. Conversely,

71. *Id.* at 33.

72. One author has suggested that commercial viability could distinguish a recombinant protein from the naturally occurring isolate by creating a legal fiction whereby a recombinant protein would be "coupled" to its method of production. Michael S. Greenfield, *Recombinant DNA Technology: A Science Struggling with the Patent Law*, 44 STAN. L. REV. 1051, 1082 (1992). The Economic Doctrine of Equivalents gives greater meaning to the concept of commercial viability so that it may be applied in all cases where the issue of infringement under the doctrine of equivalents is raised.

73. The definition of the term "obviousness," as used in this article, is discussed in greater detail *infra* text accompanying notes 81-123.

74. The definition of the term "investment," as used in this article, is discussed in greater detail *infra* text accompanying notes 124-130.

75. The definition of the term commercial viability, as used in this article, is discussed in greater detail *infra* text accompanying notes 131-139.

where the obviousness of the accused device is greater than the product of investment and commercial viability ($O > C_V \cdot I$), the device infringes under the doctrine of equivalents.

In *Hilton Davis*, the Federal Circuit emphasized the importance of the substantiality of differences between the accused device and the patent claims.⁷⁶ In determining the substantiality of the differences, the factfinder must consider "objective evidence rather than unexplained subjective conclusions."⁷⁷ Objective evidence of equivalency is not limited to the function/way/result test of *Graver Tank*, but includes any evidence relevant to the substantiality of the differences between the accused device and the patent claim.⁷⁸ In fact, the Federal Circuit stated that "neither the Supreme Court nor this court limits the types of evidence that either party may proffer in support of a factor it considers probative of infringement under the doctrine."⁷⁹ The court recognized that "the presence of such factors will depend on the way parties frame their arguments."⁸⁰ By incorporating the objective evidence of obviousness, investment in the accused device and commercial viability, the Economic Doctrine of Equivalents examines evidence that is probative of infringement under the doctrine of equivalents. Thus, the Economic Doctrine of Equivalents is a suitable means for determining equivalency under the doctrine of equivalents.

Obviousness, investment and commercial viability, as used in the Economic Doctrine of Equivalents, will next be discussed in some detail. Although the following analysis describes use of the factors in a quantitative sense, the analysis may be conducted qualitatively as well. Like the Hand Formula, the Economic Doctrine of Equivalents may be used as a construct to clarify the criteria that a court will consider in determining infringement under the doctrine of equivalents.

1. OBVIOUSNESS

Obviousness is an underlying concern of the doctrine of equivalents. Indeed, obviousness is a synonym for the "insubstantial differences" standard enunciated by the Federal Circuit in *Hilton*

76. *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1518 (Fed. Cir. 1995) (en banc).

77. *Id.* at 1519.

78. *Id.* at 1518.

79. *Id.* at 1522.

80. *Id.*

Davis.⁸¹ The Federal Circuit has described obviousness under 35 U.S.C. § 103 as analogous to infringement under the doctrine of equivalents.⁸² The *Graver Tank* Court stated that, when determining equivalence, "[a]n important factor is whether persons reasonably skilled in the art would have known of the interchangeability of an ingredient not contained in the patent with one that was."⁸³

The obviousness factor (O) ensures that only significant improvements to a patented device will be found not to infringe under the Economic Doctrine of Equivalents. The concept of obviousness used in the Economic Doctrine of Equivalents might be described as an economic test of obviousness, and differs from the obviousness concept used in determining patentability. It should be clear that I do not advocate the use of the economic test of obviousness as a standard for patent validity. Obviousness with respect to patent validity addresses whether or not patent protection is initially appropriate; the Economic Doctrine of Equivalents, in contrast, is concerned with economic investment and with the economic impact of patents and accused devices. In the following two parts, nonobviousness in the context of patentability and in the Economic Doctrine of Equivalents are each considered.

a. Nonobviousness as a requirement for patentability

The traditional test of nonobviousness is required by section 103 of the Patent Act. Section 103 provides:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.⁸⁴

This language was explicated by the Court in *Graham*,⁸⁵ which stated:

81. *Id.* at 1520. The court further explained that "those who make only insubstantial changes to a patented product or process are liable for infringement, regardless of their awareness of the patent and its disclosure." *Id.*

82. In explaining the difference between the definition of "anticipation" before and after the 1952 amendment of the Patent Act, Judge Nies observed that "[a]ll infringements of a device do not 'anticipate' [the device] Some may be infringements under the doctrine of equivalents which, if one wished to draw a parallel, is somewhat akin to obviousness." *Lewar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 748 (Fed. Cir. 1987).

83. *Graver Tank*, 339 U.S. at 609.

84. 35 U.S.C. § 103 (1988).

85. *Graham v. John Deere Co.*, 383 U.S. 1 (1966).

the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.⁸⁶

According to this test, "[o]bviousness is a legal conclusion based on factual determinations and not a factual determination itself."⁸⁷ The necessary factual determinations are: (1) the scope and content of the prior art; (2) the differences between the prior art and the invention; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness.⁸⁸ For each of these factual determinations, the inquiry must focus, as the statute requires, on "the time the invention was made."⁸⁹ That is, a court must conclude whether the claimed invention *would have been* obvious to a person of ordinary skill at the time the invention was made, not at the time of trial.⁹⁰

Under section 103, determination of obviousness requires an examination of the "art to which [the] subject matter pertains."⁹¹ The pertinent art is determined by examining the nature of the problem confronting the inventor,⁹² as well as by considering the type of skill required to understand the patent in question, and the type of art applied to the claims by the Patent Office.⁹³ Before determining the scope and content of the pertinent prior art, a court must determine whether a reference is prior art.⁹⁴ Once this legal requirement is met,

86. *Id.* at 17-18.

87. *Aktiebolaget Karlstads Mekaniska Werkstad v. United States Int'l Trade Comm'n*, 705 F.2d 1565, 1575 (Fed. Cir. 1983) (citing *General Motors Corp. v. United States Int'l Trade Comm'n*, 687 F.2d 476, 480 (Fed. Cir. 1982), *cert. denied*, 459 U.S. 1105 (1983)).

88. *See Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1535-40 (Fed. Cir. 1983).

89. 35 U.S.C. § 103 (1988).

90. *See Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1570-71 (Fed. Cir.), *cert. denied*, 481 U.S. 1052 (1987).

91. 35 U.S.C. § 103 (1988).

92. *See Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 620 (Fed. Cir.), *cert. dismissed*, 474 U.S. 976 (1985).

93. *See Orthopedic Equip. Co., Inc. v. United States*, 702 F.2d 1005, 1008 (Fed. Cir. 1983).

94. *See Panduit*, 810 F.2d at 1568. What the prior art comprises, as contrasted with what it teaches, is a question of law. *General Motors Corp. v. United States Int'l Trade Comm'n*, 687 F.2d 476, 482 n.10 (C.C.P.A. 1982), *cert. denied*, 459 U.S. 1105 (1983). Sources of prior art are mentioned in 35 U.S.C. § 102 and include prior

the court must follow certain legal standards to determine the scope and content of the prior art.⁹⁵

The factfinder must determine whether "the reference is within the field of the inventor's endeavor."⁹⁶ If so, the reference is within the scope of the prior art.⁹⁷ If not, the factfinder must then determine "whether the reference is reasonably pertinent to the particular problem with which the inventor was involved."⁹⁸ According to the Federal Circuit, a "reference is reasonably pertinent if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering [the] problem."⁹⁹ This consideration requires the factfinder to determine whether a person having ordinary skill in the art¹⁰⁰ would reasonably have expected to solve the problem facing the inventor by considering the reference in question.¹⁰¹

Before determining the differences between the prior art and the invention, the court must interpret the meaning and scope of the

knowledge or use, prior patents, prior publications, description in a prior copending patent application that ripens into a patent, prior invention, and derivation from another. 2 CHISUM, PATENTS § 5.03[3] (1994). However, "section 102 is not the *only* source of section 103 prior art." *In re Fout*, 675 F.2d 297, 300 (C.C.P.A. 1982).

95. See *Panduit*, 810 F.2d at 1568. For example, when the prior art reference is a patent, the "patent must be considered in its entirety, i.e., as a *whole*, including portions that would lead away from the invention in suit . . . ; elements of separate prior patents cannot be combined when there is no suggestion of such combination anywhere in those patents . . . and a court should avoid hindsight" *Id.* (citations omitted).

96. *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 449 (Fed. Cir. 1986).

97. See, e.g., *In re Deminski*, 796 F.2d 436, 442 (Fed. Cir. 1986).

98. *Bausch & Lomb*, 796 F.2d at 449.

99. *In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992). The court further observed:

Thus, the purposes of both the invention and the prior art are important in determining whether the reference is reasonably pertinent to the problem the invention attempts to solve. If a reference disclosure has the same purpose as the claimed invention, the reference relates to the same problem, and that fact supports use of that reference in an obviousness rejection. An inventor may well have been motivated to consider the reference when making his invention. If it is directed to a different purpose, the inventor would accordingly have had less motivation or occasion to consider it.

Id.

100. The concept of a "person with ordinary skill in the art" is discussed in greater detail *infra*, text accompanying notes 106-110.

101. *Clay*, 966 F.2d at 660.

patent claims at issue.¹⁰² This interpretation is a question of law, incorporating "the objective test of what one of ordinary skill in the art at the time of the invention would have understood the term to mean."¹⁰³ The court must consider the claimed "subject matter as a whole," rather than merely compare the claimed subject matter with the prior art.¹⁰⁴ The differences must be evaluated in terms of the whole invention, including whether or not the prior art contains "some teaching, suggestion, or incentive" to make the changes that produce the claimed invention.¹⁰⁵

In determining obviousness, section 103 requires reference to a hypothetical person of ordinary skill in the art.¹⁰⁶ This person is "presumed to be one who thinks along the line of conventional wisdom in the art and is not one who undertakes to innovate, whether by patient, and often expensive, systematic research or by extraordinary insights."¹⁰⁷ For this reason, the actual inventor's skill is irrelevant: by definition, the inventor is someone with more than ordinary skill.¹⁰⁸ The person of ordinary skill is presumed to have knowledge of all pertinent prior art, the scope and content of which the factfinder has determined.¹⁰⁹ Thus, in light of the foregoing, the appropriate "question is whether what the inventor did would have been obvious to one of ordinary skill in the art attempting to solve the problem upon which the inventor was working."¹¹⁰

102. *Markman v. Westview Instruments*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc). See *Lemelson v. Gen. Mills, Inc.*, 968 F.2d 1202, 1206 (Fed. Cir. 1992), cert. denied, 113 S. Ct. 976 (1993). When the accused device is not patented, the court may construct hypothetical claims that describe the accused device. See *Wilson Sporting Goods v. David Geoffrey & Assoc.*, 904 F.2d 677 (Fed. Cir. 1990). According to this test, a court should "visualiz[e] a hypothetical patent claim, sufficient in scope to literally cover [sic] the accused product." *Id.* at 684.

103. *Markman*, 52 F.3d at 986. In determining the meaning of the claim to one skilled in the art, the court will consider the claim language, the specification, the prosecution history and extrinsic evidence, including expert testimony. *Id.* at 979.

104. See *In re Kaslow*, 707 F.2d 1366, 1374 (Fed. Cir. 1983).

105. *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934 (Fed. Cir. 1990).

106. See *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 454 (Fed. Cir. 1985). The Federal Circuit has enunciated several criteria to consider in determining the level of ordinary skill in the art. The factfinder may consider: "(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to these problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field." *Envtl. Designs v. Union Oil Co. of Cal.*, 713 F.2d 693, 696 (Fed. Cir. 1983).

107. *Standard Oil*, 774 F.2d at 454.

108. *Id.*

109. *Id.*

110. *In re Wright*, 848 F.2d 1216, 1219 (Fed. Cir. 1988) (citing *In re Rinehart*, 531 F.2d 1048, 1055 (C.C.P.A. 1976)).

It is now well settled that "[p]rior art . . . cannot be evaluated in isolation, but must be considered in the light of the secondary considerations bearing on obviousness."¹¹¹ Such evidence "may often establish that an invention appearing to have been obvious in light of the prior art was not. It is to be considered as part of all the evidence, not just when the decisionmaker remains in doubt after reviewing the art."¹¹² Examples of objective evidence of nonobviousness include commercial success,¹¹³ prior failure,¹¹⁴ unexpected results,¹¹⁵ long-felt problem or need,¹¹⁶ copying,¹¹⁷ and independent development.¹¹⁸

b. Nonobviousness and the Economic Doctrine of Equivalents

As used in the Economic Doctrine of Equivalents, obviousness is defined as the net present dollar value of investment directly related to the problem addressed by the accused device.¹¹⁹ This investment

111. *Alco Standard Corp. v. Tenn. Valley Auth.*, 808 F.2d 1490, 1499-1500 (Fed. Cir. 1986).

112. *See Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538-39 (Fed. Cir. 1983).

113. *See Akzo N.V. v. United States Int'l Trade Comm'n*, 808 F.2d 1471, 1481 (Fed. Cir. 1986) ("Commercial success is, of course, a strong factor favoring nonobviousness.").

114. *See Panduit Corp. v. Dennison Mfg. Co.*, 774 F.2d 1082, 1099 (Fed. Cir. 1985), *vacated on other grounds*, 475 U.S. 809 (1986). Prior failure to achieve the solution accomplished by the device in question may, where a sufficient showing has been made, be "virtually irrefutable evidence that . . . [the invention] would not have been obvious to those skilled in the art when it was invented." *Id. But cf. In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983) (evidence of prior failure is less persuasive where prior party had no motivation to succeed due to satisfaction with the status quo, or where prior party was unaware of the most advanced art).

115. *See Specialty Composites v. Cabot Corp.*, 845 F.2d 981, 991 (Fed. Cir. 1988) (citing *United States v. Adams*, 383 U.S. 39, 51-52 (1966)). Where an inventor proceeds "contrary to the accepted wisdom" and succeeds, there is strong evidence of nonobviousness. *In re Hedges*, 783 F.2d 1038, 1041 (Fed. Cir. 1986) (citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540 (Fed. Cir. 1983)). In another case, one expert, upon learning of the invention, found the results so unexpected that he conducted further tests over the course of three months to confirm the results. *Burlington Indus. Inc. v. Quigg*, 822 F.2d 1581, 1583 (Fed. Cir. 1987). Others skilled in the art merely dismissed the inventor as "crazy." *Id.* at 1584.

116. *See Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 935 (Fed. Cir. 1990) (nature of problem persisting in the art and the inventor's solution are factors to be considered when determining obviousness).

117. *Windsurfing Int'l, Inc. v. AMF Inc.*, 782 F.2d 995, 1000 (Fed. Cir.), *cert. denied*, 477 U.S. 905 (1986) ("Copying the claimed invention, rather than one in the public domain, is indicative of unobviousness.").

118. *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1380 n.4 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987) ("[S]imultaneous development may or may not be indicative of obviousness . . ." Moreover, as the court noted, problems regarding simultaneous development may be resolved in an interference proceeding).

119. Anyone who has enjoyed science historian James Burke's documentary series "Connections" will immediately recognize one of the problems with this definition:

represents the resources allocated to solving a particular problem. It is a monetary representation of what knowledge society would have had without the inventor's contribution. The investment used to determine obviousness is limited to that investment which has a sufficient nexus to the problem addressed by the accused device. This measurement should also be restricted to investment that occurred up to the time that the accused device was developed. These restrictions on the investment determination prevent a wealthy patentee from fraudulently and wastefully throwing money at a problem merely to increase the obviousness factor and, thereby, increase the likelihood that an accused device will infringe under the Economic Doctrine of Equivalents. Moreover, the amount of investment should not include investment by the inventor of the accused device, as it would be unfair to use an inventor's contribution against him.

This economic test of obviousness inherently includes some of the considerations of the traditional test of obviousness used to determine patentability. For example, the factfinder must determine what problem the accused device attempted to solve, i.e., what constitutes the pertinent prior art.¹²⁰ This may be done by considering investment directed to the nature of the problem confronting the inventor of the accused device, or investment in research reasonably pertinent to the particular problem with which the inventor of the accused device was involved. Furthermore, the investment included in the calculus must have a nexus to the particular problem addressed by the accused device,¹²¹ i.e., the factfinder must determine which investments contribute to the pertinent prior art.¹²² This requirement prevents the

the complex relationship of one technological development to another (and, thus, the relationship of investment in one device to the development of another). For example, Burke described how a seemingly simple development hundreds of years ago led to a chain of developments resulting in the development of the atomic bomb. *Connections* (B.B.C. T.V. & Time-Life Television broadcast, Sept. 29-Dec. 29, 1979). This problem is addressed in the Economic Doctrine of Equivalents by requiring a nexus between the investment and the problem addressed.

120. For example, suppose the accused device is a television with an improved picture tube. The pertinent art is limited to picture tube technology, not televisions generally.

121. This is analogous to the current requirement that any commercial success proffered as objective evidence of nonobviousness be a result of the merits of the claimed invention. See *Sjolund v. Musland*, 847 F.2d 1573, 1582 (Fed. Cir. 1988). Where commercial success is due to an unclaimed aspect of the invention, the factfinder cannot infer that the commercial success is due to the merits of the claimed invention. *Id.* Similarly, where investment is not directed at the specific problem addressed by the accused device, the investment cannot be included in the calculus of the Economic Doctrine of Equivalents.

consideration of investment in research that is too attenuated from addressing the particular problem.¹²³

The economic interpretation differs from the traditional nonobviousness test in that the factfinder is not required to consider a hypothetical person of ordinary skill in the pertinent art, or what would have been obvious to that person. Moreover, once the pertinent art is determined and the aggregate investment calculated, the inquiry ends. All that is relevant is the amount of investment by others in the art: the patented device is relevant only to the extent that investment in its development contributes to industrial investment in the particular problem addressed by the accused device. Under the economic test, obviousness is concerned only with the prior art. These differences greatly simplify the determination of obviousness under the Economic Doctrine of Equivalents.

2. INVESTMENT

The idea of incorporating research investment into the determination of equivalency was intimated in *Graver Tank*. After deciding that the accused composition (a flux) infringed under the doctrine of equivalents, the Court noted that, without any evidence of independent research, "the trial court could properly infer that the accused flux is the result of imitation rather than experimentation or invention."¹²⁴ Thus, the Court indicated that the absence of research investment in a device gives rise to an inference of "practicing 'a fraud on a patent.'"¹²⁵

In *Hilton Davis*, the Federal Circuit reiterated the relevance of evidence of copying.¹²⁶ The *Hilton Davis* court relied on *Graver Tank* in

122. To continue the analogy of note 121, investment is limited to development of picture tubes and picture tube technology. Thus, investment in electrical circuitry in general, for example, is too attenuated to be included.

123. For example, it is undeniable that the invention of television depended upon the successful development of electricity; however, investment in the development of electricity would not be included because that development addresses a different problem from the problems addressed by the invention of television. The point is simply this: it is not enough for a technology to be related to the accused device; rather, the technology must address the same problem as the accused device. This blatant example demonstrates that courts will have to determine what investment may be included in the obviousness calculus: this determination, far from simple addition, will require judicial interpretation as to what constitutes relevant prior art.

124. *Graver Tank*, 339 U.S. at 612.

125. *Id.* at 618. Obviously, investment would not include, in the extreme case, expenditures for industrial espionage in order to gain information as this is a blatant example of "practicing a 'fraud on a patent.'" *Id.*

126. *Hilton Davis*, 62 F.3d at 1519.

asserting that evidence of copying is relevant to a determination of equivalence.¹²⁷ However, the court expressly stated that an inference of copying "would not dominate the doctrine of equivalents analysis. Instead, where the inference arises, it must be weighed together with the other evidence relevant to the substantiality of the differences."¹²⁸

This concern with copying is addressed by the investment factor in the equation. Evidence of copying is manifested in the Economic Doctrine of Equivalents as an absence of investment. By relating investment, whether by evidence of copying or otherwise, with other factors of equivalency, the Economic Doctrine of Equivalents satisfies the Federal Circuit's concern that such evidence not dominate the analysis. Moreover, because evidence of copying may not be black or white but may be a matter of degree, using a measure of investment to represent such evidence will allow greater accuracy in attributing the proper weight to such evidence.¹²⁹ The equation requires a court to consider *any* investment directly related to the accused device. Thus, the equation facilitates consideration of research investment when such investment is readily quantifiable.

Investment should include only those expenditures that are specifically made for the accused device. For example, purchases of raw materials consumed exclusively in the production of the device are part of the investment. The entire salary of a scientist, however, could be counted toward the investment only if that scientist worked exclusively on the device; otherwise, the portion of the salary credited to investment should be prorated based on the percentage of hours that scientist worked on the device. Thus, if the scientist spent half of his time working on the device, fifty percent of his salary may be counted as part of the investment in the device.

Inadvertent invention provides an interesting illustration of the investment factor. Suppose an inventor in a microbiology laboratory creates an economically desirable strain of bacteria that is novel and nonobvious simply by accidentally leaving the cover off a petri dish. This omission allows another substance used by the scientist to react accidentally with the culture, resulting in the new bacterium. The proper consideration of investment would include overhead investment relating to the scientist's work. By contrast, suppose a person, while rummaging through his garage, accidentally knocks over a can of

127. *Id.*

128. *Id.*

129. For example, suppose an accused device comprising five components. If four of the components are copied from a patent, only the investment (if any) in developing the fifth component is included in the calculus.

something, allowing it to mix with another substance. This accident results in the invention of a commercially desirable compound that is novel and nonobvious. In this case, there is no overhead investment in the invention. This example illustrates the meaning of relevant investment in the invention. Of course, the person in the garage, after discovering the compound, could invest in developing the material. However, the length to which one must go to create a situation where the investment factor is inconsequential serves to demonstrate the relevance of this factor in the ordinary course of invention.

By considering investment, combined with commercial viability, in the determination of infringement, the Economic Doctrine of Equivalents protects accused devices which required some effort to develop and which increase efficiency. One possible criticism of this use of investment has been noted by Edmund Kitch: the patent laws should not penalize the low-cost inventor.¹³⁰ This criticism is inapposite here. Under the Economic Doctrine of Equivalents, the focus is on whether the accused device infringes the patented device, not whether or not the accused device is worthy of patent protection. Penalizing the least-cost inventor is less of a concern when the invention is accused of infringing a device which has already been deemed worthy of patent protection.

The investment factor represents competing policies: while it is true that the patent law should not penalize an inventor for developing a device with the most efficient use of resources, neither should the patent law reward an "inventor" who has simply copied other devices and made minor changes at little cost.

3. COMMERCIAL VIABILITY

Commercial viability is defined simply as the increased efficiency created by the accused device. Increased efficiency may exist in different forms, but the underlying rationale is the same: a difference¹³¹ in the accused device that results in reduction of cost. The commercial viability factor ensures that only devices that do not increase economic efficiency infringe under the Economic Doctrine of Equivalents. This is consistent with the goal of the patent system of providing incentives for inventors to provide society with beneficial products and knowledge. Although the consideration of commercial

130. Kitch, *supra* note 26, at 281. The salient distinction is that Kitch was discussing the least-cost inventor in terms of issuing a patent, rather than infringing a patent.

131. The word "difference" in this sense means one or more alterations in the accused device that preclude the literal infringement of the patentee's claims, such as an aspect of the accused device that was in the public domain.

viability in this context does not concern the patented device, it nonetheless provides the same incentive: patentees are encouraged to claim the most efficient embodiment of their inventions, thereby reducing the likelihood that an improvement on the device will have significant commercial viability. Moreover, the commercial viability factor prevents an extension of patent scope that would preclude dissemination of products and knowledge that do not infringe the literal meaning of the patent claims and increase social welfare.

The use of efficiency as an indication of commercial viability is suggested by Professors Merges and Nelson.¹³² The Economic Doctrine of Equivalents takes this use of efficiency of the accused device one step further by requiring that the increased efficiency be quantifiable as cost savings. That is, the efficiency that commercial viability represents must be a measurable reduction in cost (e.g., the cost of production or use of the claimed device). This reduction need not merely be the reduction of production costs of *making* the accused device; any difference that results in increased efficiency is relevant and therefore is included in the calculus of commercial viability.¹³³ By contrast, a mere inference that efficiency is increased by an alteration in a device would be no more helpful to the courts than the suggestion that only significant improvements in a device will not infringe under the doctrine of equivalents.¹³⁴

The Federal Circuit noted that “[e]vidence of ‘designing around’ the patent claims is also relevant to the question of infringement

132. Merges and Nelson, *supra* note 22, at 859. The authors analyze *Texas Instruments I*, 805 F.2d 1558 (Fed. Cir. 1986), and emphasize the added increased efficiency of the accused device. *Id.* at 857-59. The authors then suggest that application of the doctrine of equivalents should include consideration of “[c]hanges in the number of components; [g]reatly improved efficiency in individual components; [and i]ncreased efficiency in the way components work together, i.e., overall design components.” *Id.* at 910.

133. For example, again suppose a simple patented device of ten components. The accused device also has ten components, five of which are identical to components in the patented device and five of which are not. The accused device performs exactly the same function in exactly the same way as the patented device. The production cost of each device is the same. But the accused device performs the task in half the time taken by the patented device. If this difference manifests itself as a cost savings to the end-user, the savings represents a cost reduction, i.e., increased efficiency and thus, commercial viability.

134. For example, suppose a simple patented device comprising ten components. The accused device performs exactly the same function, in exactly the same manner, but incorporates only five components. On the surface, the accused device appears to increase efficiency. However, if the cost of making the accused device equals the cost of making the patented device (for whatever reason), then there is no increase in economic efficiency. Therefore, commercial viability is defined as increased efficiency as measured by lower cost.

under the doctrine."¹³⁵ Not only does designing around a patent require investment, but:

[t]he ability of the public successfully to design around—to use the patent disclosure to design a product or process that does not infringe, but like the claimed invention, is an improvement over the prior art—is one of the important benefits that justify awarding the patent owner exclusive rights to his invention. Designing around “is the stuff of which competition is made and is supposed to benefit the consumer.” When a competitor becomes aware of a patent, and attempts to design around its claims, the fact-finder may infer that the competitor, presumably one of skill in the art, has designed substantial changes into the new product to avoid infringement.¹³⁶

Commercial viability is a more objective, tangible measure of designing around a patent. It is a measure, not merely an inference, of competition resulting in social benefit.

Commercial viability is expressly distinguished from commercial success.¹³⁷ Professor Merges has argued that reliance on commercial success as an indication of nonobviousness in determining patentability may lead to undesirable consequences.¹³⁸ However, there may be situations where some degree of commercial success is, at least in part, indicative of commercial viability. For example, suppose a drug accused of infringement has greater efficacy than the patented drug, but has the same production cost as the patented drug. In this case, commercial success, as measured by the greater sales of the accused drug, may be the only economic measurement of commercial viability. In cases where commercial success is a proxy for commercial viability, Professor Merges' suggestion that the underlying reasons for the commercial success be considered is applicable.¹³⁹

135. *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1520 (Fed. Cir. 1995) (en banc).

136. *Id.* (citation omitted).

137. In part, this distinction arises from the requirement that any commercial viability, i.e., increased efficiency, arise from an improvement in the device. This excludes any cost savings from other sources, such as lower labor wages. Although production of a device by cheaper labor will result in lower cost, this is not the type of economic impact to which the Patent Act is directed.

138. Robert P. Merges, *Commercial Success and Patent Standards: Economic Perspectives on Innovation*, 76 CAL. L. REV. 803 (1988). Professor Merges argues that by blindly accepting evidence of commercial success as evidence of nonobviousness, courts run the risk of rewarding nontechnical achievements, such as superior marketing techniques, distribution systems and service networks, rather than rewarding technological invention.

139. In brief, Professor Merges recommends coupling commercial success with prior failure of others or, alternatively, scrutinizing evidence of commercial success to ensure that it is probative of invention, rather than qualities that the patent system is not designed to reward, e.g., superior advertising efforts. *Id.* at 874-75. Apparently

As a practical matter, it is worth noting that the value of commercial viability may be less than, or equal to, zero. Given the mathematical relationship, either of these situations requires judgment as a matter of law for the patentee. Where commercial viability of the accused device is nil, i.e., there is no increased efficiency resulting from the accused design, the obviousness factor will necessarily be greater and infringement can be found. Similarly, where the commercial viability of the accused device is negative, i.e., there is a decrease in efficiency resulting from the accused device, the obviousness factor will again be necessarily greater.

C. Criticisms and Strengths of the Economic Doctrine of Equivalents

Initially, it may appear that the Economic Doctrine of Equivalents incorporates criteria that examine the accused device without reference or comparison to the patented device. However, application of the Economic Doctrine of Equivalents inherently accounts for the patented device. For example, the commercial viability of an accused device must be made with reference to the patented device: an increase in efficiency will be determined by comparison to the patented device. Similarly, the obviousness factor must be calculated by including the contribution of the patented device to the prior art, to the extent that such contribution is relevant.

Strictly speaking, the Economic Doctrine of Equivalents requires a change in the traditional doctrine of equivalents paradigm which compares the accused device with the patent claims. But the new paradigm posited by the Economic Doctrine of Equivalents results from consideration of the purposes of the Patent Act and the underlying reasoning of the traditional doctrine of equivalents. This new paradigm manifests itself in an economic context. Judge Newman recognized this context by stating that "[t]he patent law is directed to the public purposes of fostering technological progress, investment in research and development, capital formation, entrepreneurship, innovation, national strength and international competitiveness. Our

courts are able to distinguish between commercial success resulting from invention and that resulting from other factors: in determining obvious *vel non* under § 103, the Federal Circuit stated that "while there is evidence that marketing and financing played a role in the success of [the patentee's invention], as they do with any product, it is clear to us on the entire record that the commercial success here was due to the merits of the claimed invention." *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1383 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987).

review of the doctrine of equivalents takes place in this context, not as an abstraction insulated from commercial reality."¹⁴⁰ Thus, the essential problem with the doctrine of equivalents is not the purpose behind the doctrine but the application of it.¹⁴¹ Failure to recognize the economic context will only result in further frustration with the doctrine.

The Economic Doctrine of Equivalents emphasizes both the prior art and the accused device. On one side of the equation, the obviousness factor is concerned with investment in the prior art. On the other side, commercial viability and investment are concerned with the accused device itself. This lesser reliance on the patented device itself decreases a court's ability to expand the claims of a patent in litigation beyond what was granted by the Patent Office.

The strength of the Economic Doctrine of Equivalents is that it focuses a court's analysis on criteria that best serve the purposes of both the Patent Act and the traditional doctrine of equivalents. First, the commercial viability factor represents the goal of the Patent Act to promote the invention, development and marketing of products that are useful to society. It thus encourages development of devices where there is no literal or fraudulent infringement and where commercial viability is great. Second, the investment factor serves to ensure that the alleged infringer does not practice a fraud on a patent. This factor also brings a tangible meaning to the notion of practicing fraud on a patent.

Some may argue that simply reducing a concept to an algebraic equation does not eliminate the uncertainty inherent in the concept of equivalence. The Economic Doctrine of Equivalents, however, reduces uncertainty as compared to the traditional doctrine of equivalents because: (1) it focuses courts on the most important considerations of the doctrine and the Patent Act; and (2) it provides a method for introducing quantitative analysis into the doctrine of equivalents. But even if the formulation provided no greater certainty than the traditional methods, it does furnish courts with a more familiar manner of analysis. This will serve to overcome any apprehension judges or juries may feel when considering highly technical matters involving infringement.

The Economic Doctrine of Equivalents may also be criticized as a simple mechanical calculation where a more flexible approach is needed. This criticism mischaracterizes the Economic Doctrine of

140. *Hilton Davis*, 62 F.3d at 1536.

141. The fact that the Federal Circuit's decision in *Hilton Davis* was 6-1-5 is justification enough for a new approach to the doctrine of equivalents.

Equivalents. The Economic Doctrine of Equivalents is an almost purely objective test; but like most rules of law, it requires some interpretation for implementation. For example, the obviousness determination requires some discretion as to whether certain investment addresses the same problem addressed by the accused device. The significant increase in objectivity achieved by the Economic Doctrine of Equivalents is not strained by the possible subjectivity of the obviousness factor. Any subjectivity introduced by the obviousness factor is more than counterbalanced by the objectivity of the overall formulation. Thus, the Economic Doctrine of Equivalents is not merely a mathematical formula applied perfunctorily by courts, but is a flexible guideline for promoting the goals of the Patent Act in accordance with the true purpose of the traditional doctrine of equivalents.

One concern raised by the use of investment in the Economic Doctrine of Equivalents is that, taken together, the investment and commercial viability factors could allow a device with little commercial viability which was backed by substantial investment to evade an infringement finding. A devious inventor could obtain insurance against an infringement finding by driving up investment in a device, irrespective of any increase in commercial viability.¹⁴² Assuming for the moment that the overinvestment is the type in which a rational investor would engage, such overinvestment does not defeat application of the Economic Doctrine of Equivalents. First, if the accused device offers no increased efficiency whatsoever, i.e., the commercial viability equals zero, then no amount of investment will avoid a finding of infringement under the Economic Doctrine of Equivalents. Second, any investment which rises to the level of fraudulence may be so identified and discounted by the factfinder.¹⁴³

The Economic Doctrine of Equivalence is also likely to be criticized for requiring quantitative analysis where it is not always possible to do so. For example, while major corporations may be able to produce the information required for the analysis, a single inventor conducting research in her garage may not be able to provide detailed information, particularly where market analysis is required. It is important to emphasize that, more than anything else, the Economic Doctrine of Equivalents is a paradigm for understanding infringement

142. It is possible to dismiss the extreme case by simply stating that rational actors would not invest in this manner. Rational actors do, however, purchase insurance, so that some overinvestment to guard against potential infringement litigation is possible.

143. For example, where an inventor purchases supplies that are readily obtained at one-third the price, the factfinder would consider only the lower price.

under the doctrine of equivalents. The Hand Formula has been subject to similar criticism. But even critics of the Hand Formula will recognize that the formula is helpful in understanding the underlying considerations of negligence. So it is with the Economic Doctrine of Equivalents. Even where a quantitative analysis is not appropriate or possible (for whatever reason), the formulation provides assistance in understanding the underlying considerations of the doctrine of equivalents and the Patent Act.

As courts¹⁴⁴ and scholars¹⁴⁵ increasingly incorporate economic analysis into legal thought and interpretation, it is not surprising that traditional legal doctrines will be revised and reformulated. Where revision and reformation through economic analysis results in a more cohesive legal doctrine, courts should not hesitate to adopt new interpretations. Given the economic nature of patent law, this particularly applies to the doctrine of equivalents.¹⁴⁶ The Economic Doctrine of Equivalents does not contravene the law as it exists: it merely serves to clarify the existing analysis in a manner more accessible to courts, inventors and investors.

V. APPLICATION OF THE ECONOMIC DOCTRINE OF EQUIVALENTS

A. Application Generally

A patentee establishes a prima facie case of infringement under the Economic Doctrine of Equivalents by introducing evidence of obviousness, investment and commercial viability which demonstrates $O > C_v \cdot I$.¹⁴⁷ Once this burden is satisfied, the alleged infringer may dispute the patentee's calculus by introducing evidence to refute the

144. See, e.g., *Carlson v. Bic Corp.*, 840 F. Supp. 457, 464 (E.D. Mich. 1993). In applying the Michigan state law of negligence, the district court noted that the risk-utility test used by the state courts is "a detailed version of Judge Learned Hand's negligence calculus"

145. See, e.g., Richard H. McAdams, *Relative Preferences*, 102 YALE L.J. 1 (1992). Professor McAdams elucidated what had confounded many adherents of economic analysis: an economic model which demonstrates the efficiency of taxation and antidiscrimination laws.

146. See generally Kenneth W. Dam, *The Economic Underpinnings of Patent Law*, 23 J. LEGAL STUD. 247 (1994); Yusing Ko, Note, *An Economic Analysis of Biotechnology Patent Protection*, 102 YALE L.J. 777 (1992); John W. Schlicher, *If Economic Welfare is the Goal, Will Economic Analysis Redefine Patent Law?*, 4 No. 6 J. PROPRIETARY RTS. 12 (1992).

147. The patentee may gain access to relevant information under the rules of discovery. Any concerns regarding confidential information may be handled by the court on a case by case basis; a court may grant a protective order to prevent dissemination of critical information.

patentee's case.¹⁴⁸ As explained below, the Economic Doctrine of Equivalents should be applied in any case where infringement is alleged, whether or not literal infringement is found.

The Economic Doctrine of Equivalents places less emphasis on the protection of pioneer inventions than the traditional doctrine.¹⁴⁹ Because a pioneer invention has virtually no prior art, the obviousness factor will be relatively small. Thus, *ceteris paribus*, infringement will be more difficult to prove in the case of a pioneer invention. This is not a fundamental flaw, however, because the Economic Doctrine of Equivalents will still function to protect only socially beneficial improvements. The purpose of the pioneer invention doctrine is to afford greater protection to those inventions that are uniquely innovative. The purpose of the Economic Doctrine of Equivalents is to protect those inventions that do not literally infringe and increase efficiency. The broad protection afforded pioneer inventions becomes unwarranted where another inventor makes an improvement, as opposed to an imitation, that is truly beneficial to society, as determined by the Economic Doctrine of Equivalents. This is especially so considering that the pioneer inventor presumably has a competitive advantage. Where the pioneer inventor has the opportunity to improve upon his own invention, but another succeeds first, the doctrine of equivalents should not protect the pioneer invention at the expense of a valuable improvement. Indeed, to do so would be contrary to the purpose of the patent law.

The advantage in applying the Economic Doctrine of Equivalents is that it inherently accounts for the uniquely innovative aspects of pioneer inventions. There is no need for a court to determine whether or not an invention should receive pioneer status. Where a pioneer invention has a greater adverse effect on the commercial viability of an accused device than a non-pioneer invention, the calculus itself will account for an invention deserving of pioneer status. Moreover, the Economic Doctrine of Equivalents does not require a court to determine whether a particular patent describes a pioneer invention; rather, by measuring a device according to its particular commercial viability, the Economic Doctrine of Equivalents recognizes that pioneer status is a matter of degree.¹⁵⁰ In cases where an accused

148. For example, the alleged infringer may challenge a portion of the amount included in the obviousness calculation as being outside the scope of the prior art.

149. See *supra* text accompanying notes 51-53.

150. This is consistent with the current application of the doctrine of equivalents to pioneer inventions: "the 'pioneer' is not a separate class of invention, carrying a unique body of law. The wide range of technological advance between pioneering

device has little or no commercial viability because the patented device is simply the most efficient embodiment of the patent, that patent will, in effect, enjoy pioneer status. But where the accused device is more efficient as a result of the defendant's effort (i.e., investment), the patented device will receive a lesser degree of protection.

In a related manner, application of the Economic Doctrine of Equivalents also accounts for the reverse doctrine of equivalents. There is no need for a court to determine whether "a device is so far changed in principle from a patented article that it performs the same or a similar function in a substantially different way"¹⁵¹ so that the reverse doctrine of equivalents applies. By applying the Economic Doctrine of Equivalents even when the accused device literally infringes the patent, the defendant has the opportunity to demonstrate, in a meaningful way, that the accused device is a substantial change from the patented device. This ensures that all the purposes of the doctrine of equivalents, in light of the goals of the patent system, are served.

B. Application to *Graver Tank*

Applying the Economic Doctrine of Equivalents to the facts in *Graver Tank* yields the same result as reached by the Supreme Court. This case also illustrates that it is unnecessary to have a strict numerical basis in order to apply the formulation. In other words, it is not necessary to know the absolute value of a factor if its relative value is known. Thus, the following interpretations of obviousness, commercial viability and investment will be made by reference to the investment in the patented device.

1. OBVIOUSNESS

Although the *Graver Tank* opinion does not provide detailed information regarding investment in the relevant prior art it is possible to draw inferences from the facts given. Certainly the investment in development of the patented composition is included in the obviousness calculus. In a case such as this, where actual figures are not available, the relative magnitude of the factor is essential.

breakthrough and modest improvement accommodates gradations in scope of equivalency. . . . The place of a particular invention in this spectrum depends on all the circumstances" *Sun Studs, Inc. v. ATA Equipment Leasing, Inc.*, 872 F.2d 978, 987 (Fed. Cir. 1989) (citation omitted).

151. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 608 (1950).

Given the insubstantial change in the accused composition, the obviousness factor in *Graver Tank* is relatively great.¹⁵²

2. COMMERCIAL VIABILITY

The facts of *Graver Tank* give rise to certain inferences that may be used to determine commercial viability. First, the fact that the accused and patented compositions were "identical in operation and produce the same kind and quality of weld"¹⁵³ suggests that the accused device did not result in anything more than a negligible increase in efficiency. Second, the similarity between the two compositions—one using silicates of calcium and magnesium, the other using silicates of calcium and manganese¹⁵⁴—gives rise to the inference that the difference in production costs of the two compositions is not great. Therefore, it is likely that commercial viability is relatively insignificant.

It is worthwhile to recognize that if the facts were such that the substitution of manganese silicates for magnesium silicates resulted in a dramatic cost savings, it is possible that there would be no infringement under the Economic Doctrine of Equivalents. Under the current doctrine of equivalents analysis, a similar noninfringement finding would be possible. Such a finding would be predicated on the substantial cost savings created by the accused device—the same criterion that the Economic Doctrine of Equivalents emphasizes.

3. INVESTMENT

Certain inferences about the degree of investment in the accused device may be drawn from the facts given. The Court noted that there was no "explanation or indication that [the accused composition] was developed by independent research . . . [and] is the result of imitation rather than experimentation or invention."¹⁵⁵ Therefore, it is apparent that investment in research of the accused composition is practically nil and, thus, relatively insignificant.

4. $O > C \vee I$

Both the commercial viability and investment factors are small; obviousness, however, is relatively great. Thus, the product of

152. The Court accepted the trial court's findings that the differences in the accused device were obvious to those skilled in the art, in light of the prior art. *Id.* at 611.

153. *Id.* at 610.

154. *Id.*

155. *Id.* at 612.

investment and commercial viability is less than the obviousness factor. Even though this may not be proven quantitatively, the facts of the case allow a court to make inferences that substantiate this conclusion. Therefore, the accused composition infringes under the Economic Doctrine of Equivalents.

VI. CONCLUSION

Arising out of the Supreme Court's admonition that "[e]quivalence, in the patent law, is not the prisoner of a formula,"¹⁵⁶ the Economic Doctrine of Equivalents provides a concise, yet comprehensive, means for applying what has proved to be a troublesome doctrine. Given all the rhetoric about protecting the virtuous inventor from the scurrilous imitator who evades infringement with minor modifications, the time has come to recognize an interpretation of the doctrine of equivalents that addresses economic impact.

The rationale behind the Economic Doctrine of Equivalents reflects the legal reasoning behind both *Graver Tank* and *Hilton Davis*. These opinions provide three fundamental principles underlying the doctrine of equivalents. First, only insubstantial, obvious changes come within the purview of the doctrine. Second, where there is evidence of copying, or conversely, no evidence of investment in the accused device, application of the doctrine of equivalents is more appropriate. Third, where there is evidence that the defendant sought to design around the patent claim, application of the doctrine of equivalents is less appropriate. These principles are adequately represented in the Economic Doctrine of Equivalents by the obviousness, investment and commercial viability factors, respectively. The relation of these factors in the equation provides a rationale for the factfinder to use in the determination of infringement under the doctrine of equivalents. Thus, the Economic Doctrine of Equivalents provides a structure for determination of infringement under the doctrine of equivalents.

Equally important is the fact that the Economic Doctrine of Equivalents uses measured quantities, not inferences, to determine equivalency. The test enunciated in *Hilton Davis* describes important considerations used to draw inferences. The test enunciated in this article describes quantification of the same considerations used to make determinations. In *Hilton Davis*, Judge Newman assessed the doctrine of equivalents:

156. *Id.* at 609.

[T]he major contribution of the doctrine of equivalents is now, and always has been, to the idea of a fairer, less technocratic, more practical patent system; one that is oriented toward encouraging technologic innovation and discouraging free riding; one that is not at the "mercy of verbalism," in the words of *Graver Tank*. In this way the doctrine of equivalents can contribute a degree of added investment confidence to the inherently risky environment of new technology. However, it will not serve that function if its application is so unpredictable that it cannot be relied upon. Indeed, the determination of technologic equivalency should be reasonably predictable by not only the innovator but also the competitor. When applied to a particular patented invention, it should be reasonably predictable whether a specific device will be found "equivalent."¹⁵⁷

Because the Economic Doctrine of Equivalents relies on measurements, rather than inferences, it is more predictable than the current test for equivalency.¹⁵⁸ The formulation provides more certainty for patent attorneys in advising their clients, as well as providing commercial actors with a legal doctrine expressed in cognizable terms. As Judge Newman concluded, "[i]t is not the doctrine of equivalents, but the uncertainty of its application, that causes the uncertainty in commercial relationships."¹⁵⁹ The Economic Doctrine of Equivalents should remove the uncertainty in the application of the doctrine.

While affording the opportunity to rein in the doctrine of equivalents, the Economic Doctrine of Equivalents remains faithful to the purposes of the traditional doctrine of equivalents, as well as the patent law in general. As Judge Newman further observed, "[n]ot all improvements are equal, and neither are their implications for technological growth."¹⁶⁰ The Economic Doctrine of Equivalents takes notice of this observation and seeks to reflect it in a manner that is consistent with the traditional doctrine of equivalents. In short, the Economic Doctrine of Equivalents provides a feasible rationale for a troublesome doctrine.

157. *Hilton Davis*, 62 F.3d at 1534 (Newman, J., concurring); see also Thomas K. Landry, *Certainty and Discretion in Patent Law: The On Sale Bar, The Doctrine of Equivalents, and Judicial Power in the Federal Circuit*, 67 S. CAL. L. REV. 1151, 1202 (1994) (concluding that "[n]o one should expect the court to achieve certainty in the doctrine of equivalents").

158. This is not to say that parties working independently of each other will arrive at the same exact measurements. Like any economic model, accuracy in the result depends on accurate information. However, the Economic Doctrine of Equivalents allows for better prediction of infringement, as well as better litigation risk assessment.

159. *Hilton Davis*, 62 F.3d at 1532 (Newman, J., concurring).

160. *Id.*

It is, perhaps, appropriate that a modification of the Hand Formula be devised to clarify and apply the doctrine of equivalents. Before the *Graver Tank* opinion issued, Judge Hand had eloquently expressed the essence of the doctrine of equivalents: "after all aids to interpretation have been exhausted, and the scope of the claims has been enlarged as far as the words can be stretched, on proper occasions courts make them cover more than their meaning will bear."¹⁶¹ The doctrine of equivalents must be preserved: it ensures that protection of an inventor's ideas is not circumvented by mere words. But equally important is the ability of inventors and investors to allocate economic resources with confidence that a court will not deprive them of the benefits of their efforts. The Economic Doctrine of Equivalents satisfies both concerns.

161. *Royal Typewriter Co. v. Remington Rand, Inc.*, 168 F.2d 691, 692 (2d Cir.), *cert. denied*, 335 U.S. 825 (1948).

COMMENT

PHYSICIANS AND SURGEONS AS INVENTORS: RECONCILING MEDICAL PROCESS PATENTS AND MEDICAL ETHICS

JOSEPH M. REISMAN[†]

TABLE OF CONTENTS

I.	INTRODUCTION	356
II.	THE CURRENT DEBATE: SHOULD MEDICAL PROCESSES BE PATENTABLE?	363
	A. The Sharing of Medical Innovations.....	368
	B. Physicians' Duties to Patients Other Than Their Own.....	370
	C. Physicians' Conflicts of Interest	370
III.	PRIOR TREATMENT OF THE ETHICAL CONSIDERATIONS RAISED BY THE PATENTING OF MEDICAL PROCESSES.....	372
IV.	HISTORICAL CONTEXT OF THE CURRENT DEBATE	376
V.	A CLASSIFICATION SCHEME FOR ADDRESSING WHETHER MEDICAL PROCESSES SHOULD BE PATENTABLE	385
	A. Medical Product Claims	386
	B. Medical "New Use" Claims	389
	C. "Pure" Medical Process Claims	391
	D. The Relevant Distinction: The Inventor's Identity.....	393
VI.	A PROPOSAL: MANDATORY ASSIGNMENT OF PHYSICIANS' PATENT RIGHTS	396
	A. Patent Clearinghouses for Physician-Invented Patents.....	397

© 1995 Joseph M. Reisman.

[†] J.D. Candidate, 1996, Boalt Hall School of Law, University of California, Berkeley; Ph.D., 1993, M.S., 1989, University of California, San Diego; B.S., 1987, Yale University. In 1996, I will serve as a judicial clerk to Judge Alan D. Lourie, United States Court of Appeals for the Federal Circuit. I wish to thank Professors Robert Merges and Marjorie Shultz for their insights and advice; Anna Jarrard, Jon Traub and William Noonan for their helpful discussions; and Gary Pulsinelli and Pilar Ossorio for their useful, thorough comments. Of course, I also thank Sara Reisman for her support and patience.

B. ASCAP as a Model for the Patent Clearinghouses.....	400
VII. CONCLUSION	402

I. INTRODUCTION

Physicians should strive continually to improve medical knowledge and skill, and should make available to their patients and colleagues the benefits of their professional attainments.

—Principles of Medical Ethics,
American Medical Association, Section 2 (1971)

The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.

—U.S. Constitution, Article I, Section 8, Clause 8

In the context of medical patents,¹ the physicians' ethical canon often conflicts with the policy goals of the federal intellectual property system. Physicians' fiduciary obligations to their patients may conflict with the "instrumental" nature of the U.S. patent system because inventors are encouraged to invest in research in hopes of later extracting profits and recovering their investments through the enforcement and licensing of the patent right.² While physicians' principal concerns must be to provide the best possible care currently available for their patients,³ the patent system encourages future

1. As used in this Comment, the term "medical patent" means a patent claiming technologies with any application to the medical treatment of humans or animals. A medical patent may contain claims for (i.e., protecting) a pharmacological composition, a mechanical device (such as a splint), a method for doing surgery, a method for using a device, a series of diagnostic steps to identify disease, or any combination of such claims. A "medical process patent" contains claims for a process (such as a surgical technique), but not claims for any distinct product. For further details of the statutory definition of patentability, see *infra* part IV and accompanying notes. See also 35 U.S.C. §§ 101-112 (1988). For a relatively brief description of the requirements of patentability, see PETER D. ROSENBERG, *PATENT LAW BASICS* chs. 6-9 (1994). For a more thorough analysis, see ROBERT P. MERGES, *PATENT LAW AND POLICY: CASES AND MATERIALS* 35-587 (1992) [hereinafter MERGES, *PATENT LAW*].

2. See generally MARC A. RODWIN, *MEDICINE, MONEY, AND MORALS: PHYSICIANS' CONFLICTS OF INTEREST* (1993); MERGES, *PATENT LAW*, *supra* note 1, at 1-10. See also E. Haavi Morreim, *Blessed be the Tie That Binds? Antitrust Perils of Physician Investment and Self-Referral*, 14 J. LEGAL MED. 359 (1993); E. Haavi Morreim, *Physician Investment and Self-Referral: A Philosophical Analysis of A Contentious Debate*, 15 J. MED. & PHIL. 425 (1990).

3. The Physician's Oath, World Medical Association Declaration of Geneva, as cited in THOMAS L. BEAUCHAMP & JAMES F. CHILDRESS, *PRINCIPLES OF BIOMEDICAL ETHICS* 441 (4th ed. 1994). See also THE HIPPOCRATIC OATH, AMERICAN MEDICAL

innovation by granting inventors the right to exclude others from practicing their innovations for a limited time.⁴ For patents containing claims⁵ for medical products (e.g., pharmaceuticals and medical devices) or medical processes (e.g., new therapeutic or surgical techniques), the operation of the patent system often means that physicians will either be barred from taking advantage of recent technological advances or, at the very least, be forced to license these advances from inventors for a fee ultimately charged to the patient.

These conflicts—between enforcing ethical norms on one hand and the policies underlying patent law on the other—have been the subject of heated debate in both the medical and legal communities for over a century,⁶ and they continue to spur controversy.⁷ This

ASSOCIATION PRINCIPLES OF MEDICAL ETHICS, and THE INTERNATIONAL CODE OF MEDICAL ETHICS, *reprinted in* ROBERT M. VEATCH, *CASE STUDIES IN MEDICAL ETHICS* 351 (1979).

4. U.S. Const. Art. I, § 8, cl. 8. Under 35 U.S.C. §§ 154, 271 (1988), a patent holder may exclude others from making, using or selling subject matter claimed in the patent for 17 years from the date of issue of a valid patent. Under recently enacted legislation to bring the U.S. into compliance with the World Trade Organization's (WTO) General Agreement on Tariffs and Trade (GATT), Pub. L. No. 103-465, patent holders may exclude others for the longer of (1) 17 years from the date of issue of a valid patent or (2) 20 years from the date of filing an application with the U.S. Patent and Trademark Office (PTO) for a patent in force or one that will issue on an application filed after on or before June 8, 1995. Patents issued on applications filed after June 8, 1995 will be enforceable for 20 years from the date of filing an application with the PTO. For further details, see *Changes to Implement 20-Year Patent Term and Provisional Applications*, 58 Fed. Reg. 63,951 (1994).

5. A patent is composed, in relevant part, of a specification and one or a series of claims. The specification "shall contain a written description of the invention, and of the manner and process of making and using it." 35 U.S.C. § 112 (1988). The claims point out with particularity the "subject matter which the applicant regards as [the] invention." *Id.* Patent claims define the "metes and bounds" of the right which the patent confers on the inventor to exclude other from making using or selling the invention and have often been compared to the limits of a real property grant. ROBERT L. HARMON, *PATENTS AND THE FEDERAL CIRCUIT* 13-15 (3rd. ed. 1994).

6. In 1855, the State Medical Society of Ohio adopted the following resolution: "[I]t is not derogatory to medical dignity, or inconsistent with medical honor, for medical gentlemen to take out a patent right for surgical or medical instruments." A national association of physicians then requested that the Ohio society either rescind that resolution or sever its affiliation with the national association. William H. Edgerton, *Medical Associations and Physicians' Patent Policies*, in *THE ENCYCLOPEDIA OF PATENT PRACTICE AND INVENTION MANAGEMENT* 563 (Robert Calvert, ed. 1964); F.E. Stewart, *Is It Ethical For Medical Men to Patent Medical Inventions?*, 29 *JAMA* 583 (1897); AMERICAN MEDICAL ASSOCIATION, *PRINCIPLES OF MEDICAL ETHICS* (1905) 12, § 8 (declaring it "derogatory to the professional character for physicians to hold patents for any surgical instrument or medicines"); Morris Fishbein, *Medical Patents*, 29 *INDUS. AND ENGINEERING CHEMISTRY* 1315 (1937).

7. See, e.g., Sabra Chartrand, *A Detection Method for Breast Tumors May Add Fire to a Debate Over Patents for Medical Procedures*, *N.Y. TIMES*, Jan. 30, 1995, at D2 (Professor Michael DeGregorio, inventor of U.S. Patent No. 5,384,260 (1995), a method of detecting breast cancer tumors that develop a resistance to Tamoxifen, expressed concern over the patenting of therapeutic methods, but was obligated to pursue the

debate has recently found its way into the United States Congress. On March 3, 1995, Representatives Greg Ganske (R-Iowa) and Ron Wyden (D-Oregon) introduced new legislation which would severely limit the patentability of medical processes, and on October 18, 1995, Senator Bill Frist (R-Tenn.) introduced legislation which would allow physicians and hospitals to infringe a class of medical patents without a license.⁸ The bills, H.R. 1127 and S. 1334 respectively, are

patent and assign the patent rights to Yale University.); Edward Felsenthal, *Medical Patents Trigger Debate Among Doctors*, WALL ST. J., Aug. 11, 1994, at B1; Luran Neergaard, *Move To Patent Surgical Procedure Sparks Fight Royalties: Doctors Say Controlling the Way They Practice Medicine in Such a Way is Unethical and Drives Up Health Care Costs*, L.A. TIMES, Apr. 2, 1995, at A14. For more scholarly analyses, see William D. Noonan, *Patenting Medical Technology*, 11 J. LEGAL MED. 263 (1990) [hereinafter Noonan, *Patenting Technology*]; William D. Noonan, *Patenting Medical and Surgical Procedures*, 77 J. PAT. & TRADEMARK OFF. SOC'Y 651 (1995) [hereinafter Noonan, *Patenting Procedures*]; and George J. Annas, *Surrogate Embryo Transfer: The Perils of Patenting*, HASTINGS CENTER REPORT, June 1984, at 25 (1984).

8. On Friday, March 3, 1995, Rep. Ganske and co-sponsor Rep. Wyden introduced the following bill and submitted it to the House Judiciary Committee:

Section 1. Short Title.

This Act may be cited as the "Medical Procedures Innovation and Affordability Act."

Section 2. Limitation On Issuance Of Patents.

On or after the date of the enactment of this Act, a patent may not be issued for any invention or discovery of a technique, method, or process for performing a surgical or medical procedure, administering a surgical or medical therapy, or making a medical diagnosis, except that if the technique, method, or process is performed by or as a necessary component of a machine, manufacture, or composition of matter or improvement thereof which is itself patentable subject matter, the patent on such machine, manufacture, or composition of matter may claim such technique, method, or process.

H.R. 1127, 104th Cong., 1st Sess. (1995).

More recently, on October 18, 1995, Sen. Frist introduced the following bill and submitted it to the Senate Judiciary Committee:

Section 1. Short Title.

This Act may be cited as the "Medical Procedures Innovation and Affordability Act."

Section 2. Noninfringing Use.

Section 271 of title 35, United States Code, is amended by adding at the end thereof the following new subsection:

"(j)(1) For any patent issued on or after the effective date of this subsection, it shall not be an act of infringement for a patient, physician, or other licensed health care practitioner, or a health care entity with which a physician or licensed health care practitioner is professionally affiliated, to use or induce others to use a patented technique, method, or process for performing a surgical or medical procedure, administering a surgical or medical therapy, or making a medical diagnosis. This section does not apply to the use of, or inducement to use, such a patented technique, method, or process by any person engaged in the commercial manufacture, sale, or offer for sale of a drug, medical device, process, or

both entitled the "Medical Procedures Innovation and Affordability Act." The House bill would make a surgical, therapeutic, or diagnostic method unpatentable unless the method involved an independently-patentable pharmaceutical composition or medical device. The Senate bill, however, would simply exempt patients, physicians and other licensed health care professionals, and health care entities from patent infringement actions if the patent claims "a drug, medical device, process, or other product that is [not] subject to regulation under the Federal Food, Drug, and Cosmetic Act or the Public Health Service Act."⁹ Because, as a practical matter, medical procedures are left unregulated by these Acts, the Senate bill would make medical process patents unenforceable against typical infringers. The American Medical Association (AMA),¹⁰ along with several other

other product that is subject to regulation under the Federal Food, Drug, and Cosmetic Act or the Public Health Service Act.

"(2) For the purposes of this subsection—

"(A) the term 'device' has the same meaning as defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 321(h));

"(B) the term 'drug' has the same meaning as defined in section 201(g) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 321(g));

"(C) the term 'health care entity' means a for-profit or nonprofit entity that provides health care services, including a hospital, medical school, health maintenance organization, group medical practice, or a medical clinic;

"(D) the term 'licensed health care practitioner' means an individual other than a physician who is licensed by a State to provide health care services;

"(E) the term 'patient' means an individual who uses a patented technique, method, or process to self-administer a medical procedure, therapy, or method of diagnosis prescribed or recommended by a physician or other licensed health care practitioner;

"(F) the term 'physician' means a doctor of medicine or osteopathy or a doctor of dental surgery or medical dentistry legally authorized to practice medicine and surgery or dentistry by a State;

"(G) the term 'product' means a machine, manufacture, or composition of matter or improvement thereof;

"(H) the term 'professionally affiliated with' includes privileges, medical staff membership, employment or contractual relationship, partnership or ownership interest, academic appointment, or other affiliation under which the physician or licensed health care practitioner provides health care services (including teaching or instructional services) on behalf of or in association with a health care entity; and

"(I) the term 'State' means any State or territory of the United States, the District of Columbia, and the Commonwealth of Puerto Rico."

S. 1334, 104th Cong., 1st Sess. (1995).

9. *Id.*

10. At Supplemental Resolution 2, A-94 (§ 480.975) (1994), the AMA condemned "the patenting of medical and surgical procedures" and announced its intention to work

medical associations,¹¹ has explicitly supported the House bill and probably will support the Senate bill as well.

It should be noted that the standard of patentability proposed in the House bill resembles the standard in the European Patent Convention, in which distinct products having medical uses (e.g., pharmaceuticals or medical devices) are patentable, but surgical or therapeutic processes are not.¹² Even though the "Medical Procedures Innovation and Affordability Act" would bring domestic patent law more closely into line with the patent laws of Europe (and, indeed, the patent laws of most other countries),¹³ neither the bills' sponsors

with Congress to outlaw the patenting of such procedures. AMA Policy Compendium Supplement, June 1994, at 30. Then, in June of 1995, Dr. John Glasson, Chair of the AMA Council on Ethical and Judicial Affairs, presented the *Report of the AMA Council on Ethical and Judicial Affairs* (June 1995) (draft on file with author) [hereinafter *AMA Report*], articulating the AMA's support for H.R. 1127 (also discussed in *AMA Criticizes Patenting of Medical Procedures*, BNA HEALTH CARE DAILY, June 21, 1995, at D5 [hereinafter *AMA Criticizes*]). See also Teresa Riordan, *Patents: New Legislation Seeks to Exclude Surgical Procedures from Patent Protection*, N.Y. TIMES, Mar. 6, 1995, at D2; Brian McCormick, *Just Reward or Just Plain Wrong?: Specter of Royalties from Method Patents Stirs Debate*, 37 AMER. MED. NEWS 33 (1994) [hereinafter *McCormick, Just Reward*]; and *Bill Would Limit Issuance of Patents on Medical Procedures*, 49 PAT. TRADEMARK & COPYRIGHT J. 530 (1995) [hereinafter *Bill Would Limit*] (general discussion of legislation).

11. Riordan, *supra* note 10, at D2.

12. The European Patent Convention provides in relevant part:

Methods of treatment of the human or animal body by surgery or therapy and diagnostic methods practiced on the human or animal body shall not be regarded as inventions which are susceptible of industrial application within the meaning of paragraph 1. This provision shall not apply to products, in particular substances or compositions, for use in any of these methods.

European Patent Convention (EPC), Article 52 ("Patentable Inventions"), ¶ 4.

In EPC Article 21(1), "inventions which are susceptible of industrial application, which are new and which involve an inventive step" are defined as patentable. The proposed U.S. legislation would differ from the EPC standard in that medical process claims would be allowable, provided a distinctly patentable composition or device was "necessary" to the method.

Under the EPC standard, no such claims are allowed. This admittedly subtle distinction is discussed in part V.C., *infra*.

13. Forty-four countries, including all members of the European Patent Convention, Japan, Canada and Mexico, exclude methods of treatment of humans and animals from patentability. GATT OR WIPO? NEW WAYS IN THE INTERNATIONAL PROTECTION OF INTELLECTUAL PROPERTY, SYMPOSIUM AT RINGBERG CASTLE, JULY 13-16, 1988, IIC Studies, Annex II, p. 299. In the December 15, 1993 General Agreement on Tariffs and Trade, Including Trade-Related Aspects of Intellectual Property Rights (GATT-TRIPS), representatives of the WTO (excluding the United States) agreed to implement uniform international standards of patentability. This particular agreement generated little controversy, for the substantive standards of patentability in the developed nations are relatively uniform with the exception of medical process patents. Article 27(3)(a) of the GATT-TRIPS agreement provides that member nations "may" exclude from patentability "diagnostic, therapeutic and surgical methods for

nor the AMA cite international harmonization as a motivating factor.¹⁴

Rather, Rep. Ganske¹⁵ believes that the new law would encourage the "sharing of medical knowledge" and would promote the traditional and more natural "evolution" of medical science. He asserts that patent protection is simply not necessary to encourage the development of innovative medical procedures because medicine develops through a process of "evolution" not "revolution."¹⁶ He also asserts that medical process patents prevent innovative surgical techniques from becoming widespread.¹⁷ For this reason, he concludes that medical process patents only serve to limit physicians' options and consequently to deny patients access to the best possible medical care.¹⁸

In part II, I review and analyze the current debate over the patenting of medical processes, paying special attention to a controversial medical process patent and its physician-inventor, Arizona ophthalmologist Dr. Samuel Pallin.

Over the last decade, several commentators have addressed the concerns raised in the current debate.¹⁹ In part III, I briefly review these analyses, focusing on the commentaries by George Annas²⁰ and Gregory Burch.²¹ I also address the more recently expressed views of Timothy McCoy²² and William Noonan.²³

the treatment of humans or animals." *Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods*, 25 INT'L REV. INDUS. PROP. & COPYRIGHT L. (IIC) 209 (1994).

14. Riordan, *supra* note 10, at D2. However, Rep. Ganske did testify before the House Judiciary Committee that more than 80 countries, including most European countries, expressly prohibit medical process patents. 1995 BNA-DAILY REPORT FOR EXECUTIVES 203 (Oct. 20, 1995).

15. Rep. Ganske is also a plastic surgeon. Neergaard, *supra* note 7, at A14.

16. *Id.*; *Patient Access to Medical Procedures Strengthened in Ganske-Wyden Bill*, U.S. Congressional News Release, Mar. 3, 1995 (on file with author) [hereinafter News Release].

17. Riordan, *supra* note 10, at D2.

18. News Release, *supra* note 16.

19. See, e.g., Timothy J. McCoy, *Biomedical Process Patents: Should They Be Restricted By Ethical Limitations?*, 13 J. LEGAL MED. 501 (1992); Noonan, *Patenting Technology*, *supra* note 7; Gregory F. Burch, Note: *Ethical Considerations in the Patenting of Medical Processes*, 65 TEX. L. REV. 1139 (1987); Annas, *supra* note 7, at 25. For a more general, and thorough, analysis of the norms of science and whether they obviate the need for intellectual property protection, see Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L. J. 177 (1987) [hereinafter Eisenberg, *Proprietary Rights*].

20. See Annas, *supra* note 7.

21. See Burch, *supra* note 19.

22. See McCoy, *supra* note 19, at 508-18.

23. Noonan, *Patenting Procedures*, *supra* note 7.

In parts IV and V, I address the special role attributed to medical processes by these commentators and by the authors of the proposed legislation. Specifically, in part IV, I present an abbreviated historical overview of the changes in patent law, medical ethics, and federal regulation of medical technology over the past century. I then use these observations to reappraise the product/process distinction currently applied to medical patents by the proposed legislation. In part V, I advance a classification scheme to analyze the ethical issues raised by the types of claims typically seen in medical patents.²⁴ This scheme separates (a) medical product claims, (b) so-called "new use" claims, and (c) "pure" surgical, therapeutic, or diagnostic procedure claims. Although these categories do overlap,²⁵ each lends itself to subtly distinct ethical and legal analyses.

I conclude that no relevant distinction, whether based on medical ethics, privacy concerns, or physicians' fiduciary duties to their patients, may be drawn among the three classes of claims for medical technologies. Instead, in subpart D of part V, I assert that the only relevant distinctions among the classes lie in who has developed the innovation and in who enforces the related patent rights.

Ultimately, I assert that only when an independent physician-inventor²⁶ pursues patent protection and then owns and enforces patent rights against other physicians are the most serious ethical concerns raised. Where an institution (bound by sufficient internal and external safeguards) pursues patent rights and sees to the licensing and enforcement of those rights, the ethical concerns raised

24. For a definition of patent claims, see *supra* note 5.

25. A single medical innovation may yield a patent containing claims from all of these classes. Moreover, if a patent discloses and claims a new medical device, the inventor is entitled to claim specific uses of and techniques for employing the device that are disclosed in the specification.

It should also be noted that patent rights for a product (e.g., a pharmacological composition or a device) necessarily include the right to exclude others from any use of that product, even if a "new" use is developed by a later innovation and is independently patentable. The holder of an earlier, broader patent may "block" the holder of a later, more narrow patent from practicing the later invention, even as the holder of the later patent may "block" the earlier inventor from practicing the more narrow invention. For a more complete discussion of "blocking" patents in the context of new uses and patentable processes, see MERGES, PATENT LAW, *supra* note 1, at 182-86.

26. I have defined "independent physician-inventors" as those who are not bound by mandatory patent assignment contracts and "institutional physician-inventors" as those bound by such agreements. While this dichotomy is by no means rigid, it provides a meaningful framework from which I will draw examples. The proposal presented in part VI provides further details regarding the independent/institutional distinctions that I find most relevant.

are far less stark. This is because institutions—unlike individuals—must constantly be willing to license technologies, and thus they are far better positioned to enforce patents without harming the rights of other physicians or patients.

In part VI, I propose a system under which individual physicians would still have powerful financial incentives to develop new and useful medical innovations, but would not themselves own or enforce the rights to the patents resulting from these innovations. The proposal, based on a suggestion made over eighty years ago, would leave intact physician-inventors' ability to patent medical processes and profit from their inventions.²⁷ Under the proposal, physicians would be bound to assign patent rights either to an approved institution or to one of several national, member-run organizations subject to the oversight of the medical community. These national organizations would act as clearinghouses for the patent rights of physician-inventors,²⁸ setting rates of compensation for inventors, issuing blanket licenses for the patent rights they own and effecting efficient yet ethical means of patent enforcement. Through this mechanism independent physician-inventors would be shielded from patent-related ethical conflicts while the competing national interests in advancing medical science and in preserving physicians' ethical conduct would be served simultaneously.

II. THE CURRENT DEBATE: SHOULD MEDICAL PROCESSES BE PATENTABLE?

The two sides of the debate over the propriety of patenting medical processes represent starkly contrasting positions. The most basic factual assumption of the proponents of patentability, that the prospect of patent protection is a necessary spur for research into better and less costly medical procedures, is flatly contradicted by the opponents of patentability.²⁹ This latter group, represented by the

²⁷ Fishbein, *supra* note 6, at 1317 (discussing proposal of 1914). The proposal is also described in the Letter of A.T. Sperry, 28 J. PAT. OFF. SOC'Y 371, 372 (1946) and in ARCHIE M. PALMER, NATIONAL RESEARCH COUNCIL, SURVEY OF UNIVERSITY PATENT POLICIES: PRELIMINARY REPORT 71 (1948).

²⁸ The similarities to copyright clearinghouses such as the American Society of Composers, Authors, and Publishers (ASCAP); Broadcast Music, Inc. (BMI); and the Harry Fox Agency may be apparent to the sophisticated reader. I discuss the similarities between the proposed medical patent rights clearinghouses and ASCAP *infra* part VI.A.

²⁹ Brian McCormick, *Restricting Patents: Bipartisan Bill Would Bar Ownership Claims for Medical Methods*, 38 AM. MED. NEWS 3 (1995) [hereinafter McCormick, *Restricting Patents*]; PTO Assails Bills to Limit Patents on Medical Procedures, 50 PATENT, TRADEMARK & COPYRIGHT J. 737 (1995).

AMA and Rep. Ganske, believe that physicians should continue to rely on traditional means for appropriating the value of their inventions, such as receiving a salary or fees that reflect their accomplishments, the acclaim of their peers ("the real glory")³⁰ and the respect of their patients. These non-patent mechanisms, it is argued, provide adequate incentives to invent new processes while maintaining the incentives to disseminate new information through the medical literature.³¹ More importantly, they argue, physicians free of the confines of the patent system would also be free to abide by their fiduciary and ethical obligations to their patients.³² Furthermore, by removing the costs of enforcing and licensing patents, either version of the proposed legislation necessarily would make medical care more affordable.³³

The position taken by the AMA and supporters of the legislation may be characterized as a narrow form of the often-expressed "Principle of Non-Removal from the Public Domain."³⁴ This underlying principle of patent law dictates that all "known" technologies should be dedicated to the public domain³⁵ and that patents should not be awarded for technologies that would have been developed without the incentives of the patent system.³⁶ Of course, it is nearly impossible to determine whether a given procedure would

30. McCormick, *Just Reward*, *supra* note 10.

31. *Hearings on H.R. 1127 and H.R. 2419 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong., 1st Sess. (1995) [hereinafter *Hearings*] (testimony of Dr. Charles Kelman, President, The American Society of Cataract and Refractive Surgery) ("[T]here is little evidence that physicians and corporate investors require [the promise of significant financial rewards] to invest in research on pure medical procedures.").

32. *Id.* (testimony of Dr. H. Dunbar Hoskins, Jr., Executive Vice President, The American Academy of Ophthalmology) (Physicians are under an ethical obligation to share "their knowledge and skills for the benefit of humanity.").

33. *Id.* (testimony of Dr. Jack A. Singer) ("A Legislative response is the only effective solution to the threat that medical method patents pose to the availability, quality, and cost of health care in our country. Failure to enact the pending legislation [H.R. 1127] will do an injustice to patients and the medical profession, while contributing to exploding health care costs.").

34. HARMON, *supra* note 5, at 11-12 ("[T]he real reason for denying patent rights is the basic principle that no patent should be granted that withdraws from the public domain technology already available to the public.").

35. See 35 U.S.C. § 102 (1988) ("Conditions for patentability; novelty and loss of right to patent").

36. See 35 U.S.C. § 103 (1988) ("Conditions for patentability; non-obvious subject matter"). See also NONOBVIOUSNESS—THE ULTIMATE CONDITION OF PATENTABILITY (J. Witherspoon ed., 1980) [hereinafter NONOBVIOUSNESS] and Robert P. Merges, *Uncertainty and the Standard of Patentability*, 7 HIGH TECH. L.J. 1 (1992) [hereinafter Merges, *Uncertainty*] (concluding that one function of § 103 is to encourage research with an uncertain prospect of success at its outset).

have been developed without the patent system when a patent system is in fact in place. Supporters of the legislation simply assert that the advances in medical science prior to the availability of medical process patents indicate that patent incentives are unnecessary, while opponents of the legislation cite the large number of applications for medical process patents as evidence, however vague, of the current need for the patent incentive.³⁷

These proponents of patentability also assert that peer acclaim is rarely based on the actual value of new inventions and, moreover, that the patent system is superior to the traditional medical literature in disseminating truly novel procedures.³⁸ Additionally, they contest any assertion that the patent system sets up perverse incentives for a physician-inventor. Instead, they claim the patent system merely creates an additional cost-benefit decision for physicians and patients who wish to license the patented process but creates no notable conflicts between the interests of physician-inventors and their own patients.³⁹ Furthermore, they note that it would be "unfair" and "counterproductive" to place physicians and surgeons, unlike all other technical professionals, outside the patent system, because the incentives of the patent system have been necessary to spur developments in the medical sciences.⁴⁰ Finally, proponents of the patent system also note that whatever conflicts of interest or additional costs are introduced by the patenting of medical

37. McCormick, *Restricting Patents*, *supra* note 29, at 3; *PTO Assails Bills to Limit Patents on Medical Procedures*, 50 PAT. TRADEMARK & COPYRIGHT J. 737 (1995). See also *Hearings*, *supra* note 31 (testimony of Dr. William D. Noonan) (noting that even though U.S. patents have been issued on surgical procedures for well over a century, the economic impact of such patents is unimportant).

38. See *Hearings*, *supra* note 31 (testimony of Michael Kirk, Executive Director, The American Intellectual Property Law Association (AIPLA)) (stating that the proposed legislation would remove inventors' incentive to develop new medical processes and to disclose newly developed techniques to the public).

39. *Id.* (testimony of Michael Kirk) (noting that conflicts only arise where a physician is "unwilling to take a license under the patent" or a patentee refuses to license his rights and further noting that "[t]he proponents of [H.R. 1127] have never been able to point to any concrete examples of patients who were at risk of not having the benefits of [Dr. Samuel Pallin's] patented surgery technique").

40. *Id.* (testimony of Donald R. Dunner, Chair, Section of Intellectual Property Law, American Bar Association):

[The Section of Intellectual Property of the American Bar Association believes] that it would be unfair to single out one area of creativity—the creation of new and improved medical procedures—and deny rewards to those creators while providing them to all others. To do so would not only be unfair, but even more importantly, would be counterproductive. Our patent system and the premises upon which it is based have been tested. That testing has gone on for more than 200 years, and has produced results which are the envy of the world.

processes, these drawbacks are dwarfed by the conflicts and escalating costs inherent in the current medical environment, which includes the uncontested presence of patents covering pharmaceuticals and medical devices.⁴¹

A single independent physician-inventor appears as a focal point for both sides in the debate: Dr. Samuel Pallin, a Sun City, Arizona, ophthalmologist. In 1990, Dr. Pallin made an upside-down V-shaped incision in a patient's eye while removing a cataract but failed to stitch the incision after surgery because the patient was experiencing heart problems. To his surprise, Dr. Pallin discovered two weeks later that the scar had healed without a suture and had far less scar tissue than a normal, sutured incision.⁴² He claims to have rushed to submit an article describing this procedure to a leading journal in the field, the *Journal of Cataract and Refractive Surgery*.⁴³ The *Journal* replied that Pallin's article offered no true innovation and summarily rejected his submission.⁴⁴

Fearing that he would never be welcome in the "good old boy network"⁴⁵ of his profession, Pallin applied for and, on January 4, 1992, received U.S. Patent No. 5,080,111: "Method of Making Self-Sealing Episcleral Incision." He then offered to donate the patent to a national cataract surgeons group, but that offer was also rejected. Finally, he offered licenses to perform the patented

41. *Id.* (testimony of Dr. William D. Noonan) (although opposed to the patenting of medical processes, Dr. Noonan testified that in spite of ethical concerns raised by pharmaceuticals and medical device patents, they were justified as incentives to invest. "The need for [patent] protection is clear with biopharmaceuticals and medical devices (or methods of using them) that may require millions of dollars for research, development, FDA approval and final marketing."). *Cf. id.* (testimony of Donald R. Dunner):

Virtually the only distinction between medical methods and medical devices is that, through the ordinary course of business, medical practitioners are insulated from direct involvement with patent-liability matters in regard to medical devices. That is, the makers of medical devices typically warrant, either expressly or by legal implication, that use of the device will not infringe another's patent right. The physician is therefore indemnified. With medical method patents, in contrast, the physician is typically the direct infringer with no indemnification. However, the mere fact that physicians are exposed to the effect of the patent laws does not suggest that those laws should be limited.

42. Jodie Snyder, *A Patent for Eye Surgery? Court Case Arises Over the Technique*, THE PHOENIX GAZETTE, Apr. 4, 1995, at A1.

43. *Id.*

44. *See Hearings, supra* note 31 (testimony of Dr. Samuel L. Pallin) ("I was denied the opportunity to publish my writings and discovery in a traditional medical journal. I turned to the U.S. Patent Office to document what I had accomplished . . .").

45. Neergaard, *supra* note 7, at A14; *see also Hearings, supra* note 31 (testimony of Dr. Samuel L. Pallin).

procedure at \$3 to \$4 per surgery, asserting that the figure was quite reasonable in light of the \$17 saved by avoiding a single suture.⁴⁶ The technique is now widely performed, although few surgeons have been willing to obtain a license from Pallin.

More insulting to Pallin, however, is the fact that Dr. Jack Singer, a Vermont ophthalmologist, claims to have invented "no-stitch" cataract surgery.⁴⁷ Singer maintains that he used a related incision a month before Pallin's discovery and that he did not seek a patent because he could not ethically seek a patent covering a medical procedure.⁴⁸ Pallin counters that his procedure is different than Singer's earlier surgery and that it yields superior results.⁴⁹ He has brought a patent infringement suit against Singer and the Dartmouth-Hitchcock Medical Center in the Federal District Court for the District of Vermont,⁵⁰ vowing that if he wins, he will charge any future licensee \$5 to use his technique.⁵¹

The debate stirred by the Pallin case has generated intense rhetoric on both sides. Pallin and his supporters note that "traditional" means of sharing medical information and technical advances failed in this case and that physicians should be encouraged to explore other means of disseminating their techniques, including filing for patents.⁵² Pallin also argues that his professional skills, which lie in inventing and developing surgical techniques, should be no less rewarded by the patent law than the professional skills of chemists and engineers, whose labors routinely yield medical patents and associated licensing fees.⁵³ In broader language, members of the legal academy have joined Pallin, noting that "[t]he whole point of the monopoly of a patent is to act as an encouragement for innovation"⁵⁴ and failing to see why physicians would respond to the

46. Neergaard, *supra* note 7, at A14.

47. Snyder, *supra* note 42, at A1; Neergaard, *supra* note 7, at A14.

48. *Hearings*, *supra* note 31 (testimony of Dr. Jack A. Singer) ("I have acted in complete compliance with the AMA code of medical ethics and the report of the AMA Council on Ethical and Judicial Affairs, which concluded: '[T]he Council believes that it is unethical for physicians to seek, secure, or enforce patents on medical procedures.'"). See also *AMA Report*, *supra* note 10 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

49. Snyder, *supra* note 42, at A1.

50. *Pallin v. Singer*, No. 593CV202 (D. Vt. filed July 6, 1993), cited in *Agency Opposes Bills to Create Patent Exception for Medical Procedures*, 1995 BNA-DAILY REPORT FOR EXECUTIVES 203 (Oct. 20, 1995).

51. Neergaard, *supra* note 7, at A14.

52. *Hearings*, *supra* note 31 (testimony of Dr. Samuel L. Pallin).

53. Neergaard, *supra* note 7, at A14.

54. Riordan, *supra* note 10, at D2 (statement of Roger E. Schechter, Professor of Law, George Washington University).

incentives of the patent system any differently than other technical professionals.

Supporters of the proposed legislation, however, see Pallin as an opportunist who seeks an endless financial reward even as he admits to expending little or no effort in developing his procedure.⁵⁵ Employing even more intense rhetoric, physicians have spoken of medical process patents as leading to the Balkanization of medicine,⁵⁶ and have compared Pallin's patent to a patent for "breaking an egg into a skillet for frying,"⁵⁷ misconstruing or simply ignoring the novelty and nonobviousness standards of patent law.⁵⁸ The AMA (perhaps playing on the public's fear of escalating medical costs) has even asserted that the cost of licensing medical process patents will add significantly to our nation's medical expenses.⁵⁹

Three central issues emerge from the current debate: (1) whether the sharing of new medical techniques is currently valued in medicine, (2) whether physicians owe duties to patients other than their own (e.g., a duty to disclose innovative techniques without seeking an economic reward) and (3) whether physician-inventors, by patenting medical processes, create conflicts between their own financial interests and the interests of their patients. Though none of these issues, strictly speaking, raises questions of patent law, understanding the manner in which each is reflected in the patent law and in medical ethics may lead to a better appreciation of the conflict and, perhaps, to a suitable resolution.

A. The Sharing of Medical Innovations

The supporters of H.R. 1127 maintain that physicians are compelled by a code of ethics to share their discoveries and knowledge with other physicians.⁶⁰ This so-called "sharing norm" may be seen in the AMA's 1971 Principles of Medical Ethics: "Physicians should strive continually to improve medical knowledge and skill, and should make available to their patients and colleagues

55. See *Hearings*, *supra* note 31 (testimony of Dr. Charles Kelman, President, The American Society of Cataract and Refractive Surgery).

56. Neergaard, *supra* note 7, at A14.

57. Editorial, *Medical Greed Patently Absurd*, DAYTON DAILY NEWS, Apr. 7, 1995, at A18.

58. 35 U.S.C. §§ 102-103 (1988) (patentable invention must be both novel and nonobvious).

59. See McCormick, *Restricting Patents*, *supra* note 29, at 3; *Bill Would Limit*, *supra* note 10, at 530.

60. "[The AMA Council on Ethical and Judicial Affairs] believes that it is unethical for physicians to patent medical procedures." *AMA Report*, *supra* note 10 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

the benefits of their professional attainments."⁶¹ Similarly, the 1991 AMA Code of Medical Ethics notes that "[t]he intentional withholding of new medical knowledge, skills, and techniques from colleagues for reason of personal gain is detrimental to the medical profession and to society and is to be condemned."⁶² Of course, the meanings of "make available" and "withhold" in these contexts are subject to a variety of interpretations, but the phrase "make available to their patients" must not mean that physician-inventors are compelled to provide their services free of charge. Likewise, is offering a license to perform a patented procedure, while simultaneously publishing results in a medical journal, a way of making that skill "available"? Although an answer to this question cannot be found in the broad language of the ethical codes, perhaps the norms of the medical community provide some guidance.

The sharing norm, in the context of "basic" (not profit-yielding) research, has been addressed in great detail by Professor Rebecca Eisenberg.⁶³ She has concluded that the perspectives of the patent system and of basic research science are often irreconcilable, and that compromises should be and have been sought to accommodate the sharing of basic research information.⁶⁴ To the extent medical research may be characterized as "basic" research, her conclusions certainly apply, but they do not to the extent that research into medical processes is "applied" (profit-yielding) research. Because medical research often defies definition as either "basic" or "applied," Professor Eisenberg's observations may not provide a great deal of guidance.

Nevertheless, her concluding observation that "the patent system will influence the behavior of research scientists more effectively if it takes into account the norms and incentives that guide behavior in the scientific community"⁶⁵ may be applied to the current debate. Only by addressing the norms of the medical community may the patent system influence the behavior of physicians and surgeons to create better incentives for innovation. For this reason, a

61. AMA PRINCIPLES OF MEDICAL ETHICS § 2 (1971), reprinted in VEATCH, *supra* note 3, at 354.

62. *New Medical Procedures*, AMA CODE OF MEDICAL ETHICS: CURRENT OPINIONS AND ANNOTATIONS 139 § 9.08 (1994).

63. Rebecca S. Eisenberg, *Patents and the Progress of Science: Exclusive Rights and Experimental Use*, 56 U. CHI. L. REV. 1017 (1989) [hereinafter Eisenberg, *Patents*]; Eisenberg, *Proprietary Rights*, *supra* note 19.

64. Eisenberg, *Patents*, *supra* note 63. (To accommodate both value systems, the author suggests that a broadened "experimental use" defense to infringement be fashioned to protect basic research.)

65. Eisenberg, *Proprietary Rights*, *supra* note 19, at 230.

compromise must be struck between the concerns expressed by physicians and by the proponents of patentability if a productive change is to be made in the patent law.

B. Physicians' Duties to Patients Other Than Their Own

The question of what duty physicians might owe to patients in general, as opposed to their own patients, is also troublesome. Under the patent law, a physician-inventor who patents a medical process is certainly free to use that technique while treating any patient,⁶⁶ but other physicians must obtain (and likely pay for) a license from the patent owner if they wish to use the patented process for their own patients. For this reason, the act of patenting a new procedure can be seen as forcing a legal relationship between the physician-inventor and other physicians' patients. A question then presents itself: What legal duties, if any, arise out of this indirect relationship?

Once again, the AMA's Principles of Medical Ethics purport to provide guidance to the individual physician:

The honored ideals of the medical profession imply that the responsibilities of the physician extend not only to the individual [patient], but also to society where these responsibilities deserve [the physician's] interest and participation in activities which have the purpose of improving both the health and the well-being of the individual and the community.⁶⁷

It appears, then, that a physician owes some duty to society at large or to the local community, but it is unclear whether that duty extends to individual members of the community. Thus, assuming a physician-inventor's duty to provide for other physicians' patients, that duty squarely contradicts the perspective of the patent system. In many ways this irreconcilable conflict parallels the conflict between the sharing norm and the patent system: physician-inventors who freely share their innovations with other physicians discharge any "responsibility" to society, but *forcing* such sharing might undermine the instrumental goals of the patent system, by eliminating the economic incentives for innovation that system seeks to create.

C. Physicians' Conflicts of Interest

An undercurrent from the much larger debate over physicians' conflicts of interest is detectable in the debate over medical process

66. Subject, of course, to Food and Drug Administration (FDA) approval of the medical devices and pharmaceuticals used in the process. See *infra* part IV.

67. AMA PRINCIPLES OF MEDICAL ETHICS § 10 (1971), reprinted in VEATCH, *supra* note 3, at 354.

patents. Conflicts of interest arise most dramatically where a physician, who owes fiduciary duties to his patients, has an economic interest that creates an incentive to act against the best interests of his patient.⁶⁸ While patent rights represent but a single means by which physicians may profit at the expense of their patients' best interests, a patient's and a physician's interests may starkly contrast in the context of patent rights.⁶⁹ For example, a surgeon may use her own patented procedure and resist using a better-suited procedure if she can avoid paying a licensing fee on the "better" alternative. A related conflict, between a physician's research directed toward a patent and a patient's right to know the physician's motives, was at issue in *Moore v. Regents of University of California*.⁷⁰

In *Moore*, plaintiff John Moore was successfully treated for hairy-cell leukemia by Dr. David Golde of the University of California at Los Angeles (UCLA) Medical Center. Golde, collaborating with other UCLA researchers, developed a valuable cell line from Moore's T-lymphocytes and obtained, for the University, a patent for the purified cell line. Neither Golde nor any of Moore's physicians disclosed the extent of the ongoing research or their developing economic interest in the outcome of that research, even as they continued to withdraw samples of Moore's "blood, blood serum, skin, bone marrow . . . and sperm" for reasons related *only* to the development of the purified cell line. The court, determining that Golde had entered into a "fiduciary"⁷¹ relationship with Moore by agreeing to treat his disease, held "a physician who is seeking a patient's consent for a medical procedure must, in order to satisfy his fiduciary duty and to obtain the patient's informed consent, disclose

68. RODWIN, *supra* note 2. The author notes: "There are two main types of conflict of interest: (1) conflicts between the physician's personal interests (often financial) and the interests of the patient and (2) conflicts that divide a physician's loyalty between two or more patients or between a patient and a third party." *Id.* at 9. The conflicts of interest that arise from physicians applying for and receiving patents are almost exclusively financial conflicts of interest. The present analysis is, accordingly, limited to financial conflicts of interest.

69. *Id.*

70. 793 P.2d 479 (1990).

71. *Id.* at 485 n.10. The court cautioned:

In some respects the term "fiduciary" is too broad. In [the context of this case] "fiduciary" signifies only that a physician must disclose all facts material to the patient's decision. A physician is not the patient's financial adviser . . . [T]he reason why a physician must disclose possible conflicts is not because he has a duty to protect his patient's financial interests, but because certain personal interests may affect professional judgment.

Id. The same limitations on the use of the term "fiduciary" should be applied to this Comment.

personal interests unrelated to the patient's health, whether research or economic, that may affect [the physician's] medical judgment."⁷²

Thus, under the *Moore* standard, potential conflicts of interest arising from physician-inventors' patents or patent applications may be largely resolved by mandating that physicians fully disclose to their patients any interests in medical patents while obtaining informed consent. Nevertheless, it is still unclear whether full disclosure would require an accounting of patent applications filed, patents held, or both. Furthermore, the developing jurisprudence of physician conflict of interest does not squarely address whether medical process patents should be granted.⁷³ Instead, it only indicates that physician-held patents create an opportunity for the interests of the physician and those of the patient to diverge. Thus, physician-held patents may be seen as creating yet another economic incentive, in a growing list, for physicians to act against the best interests of their patients.⁷⁴

Neither the rhetoric surrounding the current debate nor the underlying questions that emerge provide easy answers to our central inquiry: whether medical processes should be patentable. This uncertainty arises primarily because it is impossible to know whether patent protection is necessary to spur medical invention or whether a physician's patent rights would, even with appropriate safeguards, necessarily interfere with her duties as the fiduciary of her patients. Because of this uncertainty, the analyses of the ethical (part III) and historic (part IV) perspectives on the patenting of medical processes become crucial to understanding and reconciling the seemingly irreconcilable positions in the current debate.

III. PRIOR TREATMENT OF THE ETHICAL CONSIDERATIONS RAISED BY THE PATENTING OF MEDICAL PROCESSES

Before assessing the ethical concerns raised by the patenting of various medical technologies, it is essential to review the landscape of medical ethics and, more importantly, the recent analyses of the patent system's effect on this landscape. Several law reviews have presented articles that discuss the role of patents in medicine.

72. *Id.* at 485.

73. See RODWIN, *supra* note 2, at 212-47 (asserting that disclosure is an effective remedy for conflicts of interest, but even stricter regulatory standards for avoiding conflicts should be applied to the medical community). See also E. Haavi Morreim, *Physician Investment and Self-Referral: A Philosophical Analysis of a Contentious Debate*, 15 J. MED. & PHIL. 425 (1990).

74. See Morreim, *supra* note 73.

However, no leading text in the field of medical ethics squarely addresses the issues raised by patents claiming medical advances.⁷⁵ Nonetheless, the literature of medical ethics provides an appropriate general vocabulary for discussing the ethical concerns raised by medical patents. The terminology used by Beauchamp and Childress in *Principles of Biomedical Ethics*⁷⁶ offers a useful frame of reference by dividing the ethical landscape into five broad, overlapping categories:⁷⁷ respecting patient autonomy,⁷⁸ avoiding maleficence,⁷⁹ allowing for beneficence,⁸⁰ serving justice,⁸¹ and preserving these essential elements in the physician-patient relationship.⁸² As further analysis will reveal, patient autonomy, avoiding maleficence (in the guise of physician conflict of interest), and the physician-patient relationship are most likely to be influenced by medical patents. In addition to these concerns, medical patents may create conflicts between physicians' financial incentives and the interests of the patient,⁸³ while the enforcement of medical patents may compromise a patient's rights to privacy.⁸⁴

Recent commentaries on the patentability of medical processes have also used this framework, though each author values different ethical criteria. In *Biomedical Process Patents: Should They Be Limited By Ethical Limitations?*,⁸⁵ Timothy McCoy questions the role medical

75. See, e.g., TOM L. BEAUCHAMP & JAMES F. CHILDRESS, *PRINCIPLES OF BIOMEDICAL ETHICS* 441 (4th ed. 1994). The authors dedicate 12 pages in this 500-page treatise to "The Dual Role of Physician and Investigator," but do not discuss the patenting of an invention derived from such an investigation.

76. *Id.* See also STEPHEN G. POST, *INQUIRIES IN BIOETHICS* 1-7 (1993); VEATCH, *supra* note 3, at 59-136. Veatch, unlike Beauchamp and Childress, divides the field into four categories: duty to patient and society, health-care delivery, confidentiality, and truth-telling.

77. A recently published case book for the study of the legal issues of biomedicine has adopted this framework. See BARRY R. FURROW ET AL., *HEALTH LAW: CASES MATERIALS AND PROBLEMS* (1991). The authors dedicate entire chapters to "The Relationship of Provider and Patient" and "Access to Health Care." It should, however, be noted that this classification of ethical issues does not overlap with the classification scheme of the American College of Healthcare Executives' Code of Ethics. MARC D. HILLER, *ETHICS AND HEALTH ADMINISTRATION* 120 (1986). For further discussion of the ethical concerns that inform the decisions of health care administrators, as opposed to those of physicians, see *infra* part V.D.

78. BEAUCHAMP & CHILDRESS, *supra* note 75, at 120 (1986).

79. *Id.* at 189.

80. *Id.* at 259.

81. *Id.* at 326.

82. *Id.* at 395.

83. See generally RODWIN, *supra* note 2. See also *supra* part II.C.

84. See Jeffrey A. Taylor, Comment, *Medical Process Patents and Patient Privacy Rights*, 14 J. COMP. & INFO. L. 131 (1995).

85. McCoy, *supra* note 19.

patents play in limiting patients' access to health care⁸⁶ and information transfer,⁸⁷ while also discussing the impropriety of patenting living organisms.⁸⁸ Access to health care most directly triggers concerns for patient autonomy, justice and the physician-patient relationship. The "information-sharing ethic" cited by McCoy resembles the above-mentioned "sharing norm."⁸⁹ McCoy's third concern, whether living organisms should be patented, is generally not raised by medical process patents, and accordingly finds few parallels in the ethical scheme of Beauchamp and Childress.⁹⁰ Ultimately, McCoy concludes that the role patent protection plays in medical innovation simply outweighs any ethical concerns because patent protection creates an invaluable incentive to develop necessary medical technologies.⁹¹ In light of the heightened tenor of the current debate, however, ignoring the ethical concerns raised by the medical community may not be considered a viable option.⁹²

In *Ethical Considerations in the Patenting of Medical Processes*,⁹³ Gregory Burch discusses the controversial patent covering surrogate embryo transfer (SET)⁹⁴ (a reproductive technology that is controversial in its own right)⁹⁵ and ultimately focuses on the effect the patent might have on physician-patient relationships⁹⁶ and physician autonomy.⁹⁷ He concludes that the current patent law provides inadequate safeguards for physician autonomy and suggests that a mandatory licensing scheme for medical process patents would address this inadequacy.⁹⁸ While the approach does attempt to

86. *Id.* at 510-12, 519.

87. *Id.* at 512-14, 519.

88. *Id.* at 515-17.

89. See *infra* part II.A.

90. Cf. Robert P. Merges, *Intellectual Property in Higher Life Forms: The Patent System and Controversial Technologies*, 47 MD. L. REV. 1051 (1988) [hereinafter Merges, *Controversial Technologies*] (arguing that patent law is not the appropriate arena in which to regulate new lifeforms).

91. McCoy, *supra* note 19, at 518-19.

92. But see Noonan, *Patenting Procedures*, *supra* note 7, at 663 (noting that medical process patents have had little practical effect on domestic health care delivery and suggesting that such patents will never become more than "an occasional curiosity").

93. Burch, *supra* note 19.

94. See also Maria Bustillo et al., *Nonsurgical Ovum Transfer as a Treatment in Infertile Women: Preliminary Experience*, 251 JAMA 1171 (1984); Fern S. Chapman, *Going for Gold in the Baby Business*, FORTUNE, Sept. 17, 1984, at 41.

95. For a more thorough discussion of the ethical issues raised by SET and related technologies, see Annas, *supra* note 7, at 25.

96. Burch, *supra* note 19, at 1154-59.

97. *Id.* at 1152-54.

98. *Id.* at 1169-71.

strike a compromise, it merely forces the inevitable debate over each particular "reasonable royalty" into a court, while ignoring the United States patent law's traditional avoidance of mandatory licenses.⁹⁹

In an earlier and briefer analysis of the patenting of SET techniques, George Annas (in contrast to Burch) places a special emphasis on the invasions of patient privacy *and* on the confidential physician-patient relationship, concerns which the mere enforcement of medical process patents could compromise.¹⁰⁰ Although he admits that the prospect of patent protection was essential in generating financing for the SET research,¹⁰¹ he notes that the "subject matter" of such an advanced medical procedure "does not lend itself to patent infringement enforcement without potentially unbearable privacy violations."¹⁰² Annas then concludes that patent applications claiming these procedures should be rejected unless the applicant provides a means of enforcement that will not compromise patients' privacy rights. Jeffrey Taylor, in his Comment *Medical Process Patents and Patient Privacy Rights*, proposes just such a enforcement mechanism.¹⁰³ He suggests that Congress may revise the Patent Act to allow better access to medical records (while preserving patient privacy) during enforcement of medical process patents. For example, he suggests that removing a patient's identity from medical records subject to civil discovery in a patent infringement action would protect the patient's privacy and obviate the need for informed consent.¹⁰⁴ While this proposal might address patients' rights to privacy, it

99. In this country, only the Clean Air Act of 1970 provides for mandatory licensing of patented technology between private parties. 42 U.S.C. §§ 7401-7671 (1988). This mandatory licensing scheme, however, was only created to "curtail the tendency of patents to create a monopoly on a technology that facilitates compliance with the Act." Burch, *supra* note 19, at 1168. Furthermore, mechanisms already exist to prevent patentees from refusing to license technologies required by society. See, e.g., *Vitamin Technologists v. Wisconsin Alumni Research Foundation*, 146 F.2d 941, 944-45 (9th Cir. 1944) (*cited in* *Kearns v. Chrysler*, 32 F.3d 1541, 1551 (Fed. Cir. 1994)) (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose).

100. Annas, *supra* note 7, at 25.

101. *Id.* at 25-26.

102. *Id.* at 26. For example, Annas envisions private investigators or paid informants being used to monitor the SET process.

103. Taylor, *supra* note 84, at 147.

104. *Id.* Montana and Washington have recently enacted modified versions of the 1985 UNIFORM HEALTH-CARE INFORMATION ACT to protect the confidentiality of medical records. MONT. CODE ANN. §§ 50-16-501 to 553 (1987) (Uniform Health Care Information); WASH. REV. CODE ANN., §§ 70.02.005-904 (West 1991) (Medical Records-Health Care Information Access and Disclosure).

does not address the medical community's "sharing norm," patients' autonomy, and the potential conflicts of interest raised by physician-owned patents.

Annas' and Taylor's observations do provide an effective counterpoint to McCoy's. They assert that privacy rights simply outweigh any valid patent policy in the context of medical process patents, while McCoy asserts that the underlying policies of the patent system simply outweigh any ethical concerns. Burch, perhaps seeking a compromise, proposes a mandatory licensing scheme. But such a licensing scheme does not address Annas' assertion that enforcement of patent rights will necessarily violate patients' rights to privacy. Even if licenses were granted to all interested physicians and patients, the patent holder would be obliged to monitor operating rooms to prevent others from avoiding the (mandatory) licensing fee. It appears, then, that an alternative compromise is required to strike a meaningful balance between the principles of medical ethics and the underlying policies of the patent system.

Although each author presents compelling arguments and sound reasons to examine the ethics underlying medical process patents, each assumes that medical processes raise ethical issues distinct from those raised by medical products. Quite surprising, then, is the observation that the commentators often sweep analyses of several controversial *product* patents into their analyses of the underlying ethical questions raised by medical *process* patents. It is precisely the ease with which a discussion of medical process patents can become a discussion of medical product patents that necessitates the reassessment of ethical considerations raised by medical *process* patents, per se. In the following part, I review the major historical developments in medical ethics and patent law that have led to the controversy that today surrounds medical process patents. By tracing these developments before discussing the various ethical issues raised by each class of medical patent claims, I hope to clarify the distinctions (valid or otherwise) that have led to the current controversy.

IV. HISTORICAL CONTEXT OF THE CURRENT DEBATE

Since its inception, the U.S. patent system has served one Constitutionally mandated goal: to promote science and the useful arts.¹⁰⁵ The Patent and Trademark Office (PTO), begun as the Patent

105. U.S. CONST. art. I, § 8, cl. 8. This clause also empowers the Congress to establish a system of copyrights.

Administration under the direction of Thomas Jefferson in 1790,¹⁰⁶ has served this goal by issuing patents on worthy applications, while the federal courts have played their role by selectively enforcing or invalidating issued patents and reviewing PTO decisions.

Both the PTO and the courts, under statutes ranging from the Patent Act of 1793 (written by Jefferson) to the Revised Statutes of 1874 and the Patent Act of 1952,¹⁰⁷ have applied a "three-level" filter to distinguish inventions and discoveries worthy of patent protection from those not worthy.¹⁰⁸ To pass through the first level, the applicant must show that the claimed invention belongs among those advances that, if rewarded with a monopoly, would "promote science and the useful arts." This inquiry determines whether the application claims so-called "patentable subject matter" under 35 U.S.C. § 101 and its precursor statutes.¹⁰⁹ For example, fundamental principles, laws of nature and mathematical formulae have consistently been held not patentable subject matter because issuing monopolies for such advances might stifle scientific progress. However, mechanical devices, compositions of matter, and useful processes have, more or less consistently, been held to be patentable.¹¹⁰

Second, the applicant must demonstrate that the claimed invention is novel, that no one else has previously made the invention,¹¹¹ because rewarding a second "inventor" would not serve to promote science. Third, the applicant must show that the claimed invention is technically worthy of a patent, rather than the routine exercise of one having ordinary skill in the art. This rather ambiguous, court-made standard was long termed "the standard of invention" and was finally codified in 1952 as 35 U.S.C. § 103. It is now known as the standard of "nonobviousness."¹¹²

106. P.J. Federico, *Operation of the Patent Act of 1790*, 18 J. PAT. OFF. SOC'Y 237 (1936).

107. The current Title 35 of the U.S. Code largely resembles the Patent Act of 1952. PTO regulations may be found at 37 C.F.R. For information regarding current organization and policies of the PTO (all provided by the PTO), see "<http://www.uspto.gov>" on the World Wide Web.

108. For a more thorough description of these three "basic" standards of patentability, see MERGES, *PATENT LAW*, *supra* note 1, at 36-42.

109. Prior to the Patent Act of 1952, all the requirements of patentability were codified as § 4886 of the Revised Statutes.

110. 35 U.S.C. § 101 (1988).

111. 35 U.S.C. § 102 (1988).

112. 35 U.S.C. § 103 (1988) ("Conditions for Patentability; Non-Obvious Subject Matter"). See also NONOBLVIOUSNESS, *supra* note 36; Merges, *Uncertainty*, *supra* note 36 (concluding that one function of § 103 is to encourage research, the success of which was uncertain at its outset).

Atop this three-level filter, both the PTO and the courts have imposed barriers meant to serve more flexible ethical and public policy concerns. These concerns, though rarely raised today,¹¹³ were often manifest as a "beneficial utility" requirement.¹¹⁴ In several notable opinions ranging into the early twentieth century, the PTO and the courts denied applications for otherwise patentable devices because these devices (e.g., a coin-return device for a slot machine¹¹⁵ and a random-selecting machine for distributing toys¹¹⁶) were potentially "injurious to the morals, health, or good order of society."¹¹⁷ However, as the Food and Drug Administration (FDA)¹¹⁸ and various other administrative agencies designed to safeguard the public became more influential, the roles of the PTO and of the patent law in protecting public morals and health have diminished.¹¹⁹

An understanding of the evolving standards of patentability is essential to resolving the current debate over medical process patents. The principal argument advanced by the AMA and other proponents of the legislation is that medical processes should not pass the first filter, because granting patents for such processes—in light of physicians' ethical duties to share their innovations—is simply not necessary to spur the progress of medical science.¹²⁰ So, by granting patents for such processes, the Patent and Trademark Office (PTO) is not fulfilling its Constitutional mandate to promote science and the useful arts. The other arguments against patentability, which focus

113. In their role as courts of equity, the federal courts grant preliminary injunctions against alleged patent infringers only after considering four factors: (1) the relative rights and hardships of the parties, (2) the likelihood of ultimate success, (3) the possibility of irreparable harm, and (4) the public interest. See, e.g., *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858 (Fed. Cir.), cert. denied, 469 U.S. 856 (1984); *Datascope Corp. v. Kontron Inc.*, 786 F.2d 398 (Fed. Cir. 1986).

114. *Bedford v. Hunt*, 3 F. Cas. 37 (C.C.D. Mass. 1817). For a more general discussion, see MERGES, *PATENT LAW*, *supra* note 1, at 154-59.

115. *Schultz v. Holtz*, 82 F. 488 (N.D. Cal. 1897).

116. *Meyer v. Buckley Mfg. Co.*, 15 F. Supp. 640, 641 (N.D. Ill. 1936).

117. *Reliance Novelty Corp. v. Dworzek*, 80 F. 902, 904 (N.D. Cal. 1897).

118. As the proponents of S. 1334 have noted, neither the FDA nor any other government agency regulates medical procedures. See *supra* note 8 and accompanying discussion. A vast array of information regarding the FDA's history and current policies is available on the World Wide Web at "<http://www.fda.gov>."

119. *In re Brana*, 51 F.3d 1560, 1564 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995) and holding that the PTO may not make a prima facie finding of lack of utility for a claimed antitumor agent under the implicit utility requirement of 35 U.S.C. § 112, ¶ 1, where the applicant provides only *in vivo* murine clinical data and disapproving PTO's actions requiring explicit evidence of efficacy in human clinical trials as an encroachment on the regulatory expertise of the FDA and an unfair burden on applicants for pharmacological inventions).

120. *Hearings*, *supra* note 31 (testimony of Dr. Jack A. Singer).

on ethical and conflict-of-interest norms,¹²¹ though persuasive in their own right, are reminiscent of the now disfavored "beneficial utility" standard. For this reason, and because agencies other than the PTO now fulfill the role once served by the "beneficial utility" standard, these arguments against patentability should be carefully scrutinized.

The following analysis discusses the evolving standard of patentability for medical processes, the corresponding changes to the AMA's ethical code and the development of the FDA. In it, I attempt to place the current debate in context, aiding an evaluation of the various rhetorical and ethical objections to medical process patents.

While patents have been occasionally issued on medical processes since as early as 1846,¹²² the current law of medical process patents may be traced to developments in the late nineteenth century. In an 1883 decision, *Ex parte Brinkerhoff*,¹²³ the Commissioner of the Patent Office denied an application for a patent claiming a method of treating hemorrhoids.¹²⁴ The Commissioner noted that although new pharmaceutical compositions had long been considered patentable, "the methods or modes of treatment of physicians of certain diseases are not patentable."¹²⁵ The Commissioner based this conclusion on the observation that patentable discoveries, in a majority of cases, must:

accomplish certain results, but no particular method or mode of treatment under all circumstances, and in all cases will produce upon all persons the same result, and, hence to grant a patent for a particular mode of treatment would have a tendency to deceive the public by leading it to believe that the method therein described and claimed would produce the desired and claimed result in all cases.¹²⁶

In essence, the Commissioner found that medicine was neither advanced nor precise enough as a science to grant a patent in the field. The imprimatur of the PTO would unnecessarily confuse the public by suggesting that medical science was, in fact, predictable. He then held that medical processes, per se, were not patentable subject matter because of their inherent unpredictability.¹²⁷ Patents

121. See *supra* parts II.B and II.C.

122. U.S. Patent No. 4,848 (1846) (method of using inhaled ether as anesthetic).

123. 24 Comm'r Manuscript Dec. 349 (Case No. 182, July 5, 1883), reprinted in 27 J. PAT. OFF. SOC'Y. 797 (1945).

124. See I.J. Fellner, *Patentability of Therapeutic Methods*, 28 J. PAT. OFF. SOC'Y 90 (1946) [hereinafter Fellner, *Therapeutic Methods*].

125. 27 J. PAT. OFF. SOC'Y at 798.

126. *Id.*

127. *Id.*

must be reserved for only the "well-understood" arts, such as mechanics or chemistry.

At the time, such a ruling generated little controversy in the medical community. The specter of the so-called "patent medicines," typified by magical elixirs and merchants making wholly unsupported claims regarding their products,¹²⁸ loomed over the developing medical profession. This specter threatened to undermine the profession's status.¹²⁹ The medical community, in an effort to consolidate power and project a positive public image,¹³⁰ condemned any physician who "employ[ed] . . . the methods of charlatans," dealt in secret "nostrums," or merely offered "certificates attesting to the efficacy of secret medicines, or other substances used therapeutically."¹³¹ The 1905 AMA Principles of Medical Ethics also condemned the patenting of any surgical instrument or medicine by a physician as "derogatory to the professional character."¹³²

At the beginning of the twentieth century, the U.S. Congress twice (in 1902 and 1903) failed to enact legislation that would have made medical processes unpatentable.¹³³ However, by enacting the Federal Food & Drugs Act of 1906,¹³⁴ Congress did create the Food and Drug Administration (FDA).¹³⁵ Although the early FDA had little actual regulatory authority,¹³⁶ its creation signaled the eventual demise of the "beneficial utility" standard for medical patents. With the FDA's special expertise in ensuring the safety and efficacy

128. PAUL STARR, *THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE* 79-144, (1982) (chapter entitled "The Consolidation of Professional Authority, 1850-1930"). For specific examples of advertisements promoting "patent medicines," see ALBERT S. LYONS & R. JOSEPH PETRUCCELLI, *MEDICINE: AN ILLUSTRATED HISTORY* 506-07, 527, (1987) (displaying at 506-07 advertisements for, among others: "Dr. C.V. Girard's Ginger Brandy"; "No-To-Bac," a cure for nicotine addiction; and "Hood's Sarsaparilla"; and describing at 527 the success of "Dr. James's Fever Powder," a powder composed primarily of elemental antimony).

129. I leave it to the reader to decide whether confusion between "patent medicines" and "medical patents" still influences the debate over the patentability of innovations in the medical sciences.

130. STARR, *supra* note 128, at 88-92.

131. AMA PRINCIPLES OF MEDICAL ETHICS 12, §§ 7-8 (1905) ("Patents and Secret Nostrums").

132. *Id.* § 8.

133. Noonan, *Patenting Procedures*, *supra* note 7, at 654 (1995).

134. Federal Food and Drugs Act of 1906, Pub. L. No. 59-384, 34 Stat. 768 (amended 1934). See generally "<http://www.fda.gov>" on the World Wide Web.

135. For a general discussion of the role of the FDA, see Barry S. Roberts, *Regulatory Update: The FDA Speeds Up Hope for the Desperately Ill and Dying*, 27 AM. BUS. L.J. 403 (1989).

136. For example, under the Federal Food & Drugs Act of 1906, the FDA could not test medications for safety or efficacy until they had entered interstate commerce. Such delayed testing was often too late to allow the FDA to protect consumers.

of medicines, the PTO's role as guarantor of the efficacy of patented devices and processes could be, and eventually was, limited.

Into the early twentieth century, physicians continued to pursue patent protection for their innovations, despite the pronouncement of *Ex parte Brinkerhoff*, the stated policy of the AMA, and a still-ineffectual FDA. Such patents were occasionally granted, even for medical processes. In a 1930 decision, *Dick v. Lederle Antitoxin Laboratories*,¹³⁷ a district court upheld patent claims for a method of diagnosing susceptibility to scarlet fever.¹³⁸ The *Dick* court noted the diagnostic method's reproducible results and its acknowledged value in the medical community as reasons to disregard, in this case, the general prohibition of medical process patents.¹³⁹

The late 1930s marked the emergence of the FDA as a viable and effective regulatory agency. In response to the "Elixir of Sulfanilamide" tragedy of 1937,¹⁴⁰ Congress enacted the Food, Drug & Cosmetic Act of 1938.¹⁴¹ This legislation empowered the FDA to require proof of safety before approving any medication for the market, and it gave the FDA authority to enforce its decisions by inspecting and regulating interstate commerce.¹⁴² The growing power of the FDA was seen at the time as an effective complement to the PTO's regulatory efforts.¹⁴³

Soon thereafter, in the mid-1940s, a debate over the patentability of medical processes re-emerged among patent lawyers.¹⁴⁴ While a part of this debate concerned the larger issue of

137. 43 F.2d 628 (S.D.N.Y. 1930).

138. The patent in *Dick* is an excellent example of a medical patent claiming both a product and a process for using the product (the diagnostic method). Under the proposed legislation, H.R. 1127, all the claims in such a patent would be allowable, provided they met the requirements of patentability. See *supra* note 8.

139. *Dick*, 43 F.2d at 631.

140. Arthur H. Hayes, Jr., *Food and Drug Regulations After 75 Years*, 246 JAMA 1223, 1224 (1981) (discussing how, in 1937, a Tennessee manufacturer introduced a sulfa drug in liquid form which contained highly toxic diethylene glycol. The FDA conducted no safety tests prior to marketing, and at least 107 persons died after ingesting the drug).

141. 52 Stat. 1040 (1938) (currently codified at 21 U.S.C. §§ 301-392 (1994)).

142. 52 Stat. 1040, 1052, 1057. In 1976, the FDA was also empowered to regulate the sale of medical devices. However, the FDA still does not regulate the use of medical or surgical processes. CHIEF EXECUTIVE'S NATIONAL PERFORMANCE REVIEW OF THE FDA, Apr. 6, 1995, available at "<http://www.fda.gov/po/reinvent.html>" on the World Wide Web.

143. Sperry, *supra* note 27, at 371-72 (noting that the evils of "patent medicines" had been ably mitigated by the Pure Food & Drug Act and the PTO, as well as the medical profession's efforts to stigmatize medical patents).

144. Fellner, *Therapeutic Methods*, *supra* note 124. Four letters responding to the Fellner article were also published in the Journal of the Patent Office Society during 1946: Letter of George Benjamin, 28 J. PAT. OFF. SOC'Y 369; Letter of A.T. Sperry, 28 J.

whether processes, per se, should be patentable, the unique issues raised by medical processes attracted special attention. One patent attorney contended that the underlying holding of *Brinkerhoff* (that medicine was not a precise science) was untenable in the light of "modern" medical advances, and suggested that a per se rule against medical process patents delayed progress.¹⁴⁵ His arguments elicited responses not unlike those seen today. These responses ranged from the uncompromising—"[t]he sphere of medical patents does *not* include medical applications . . . This is all. This principle has to be maintained."¹⁴⁶—to the now familiar concerns for physician autonomy—"[t]he physician should be equally free to perform any therapeutic methods which his skill and education indicate."¹⁴⁷

Meanwhile, in *Martin v. Wyeth, Inc.*,¹⁴⁸ a district court withdrew from the holding in *Dick* by invalidating a claim for a method of treating mastitis in cows. The court proclaimed that medical process patents were contrary to the physicians' ethical code and thus contrary to the public interest, even as it invalidated the patent on other grounds. At about the same time, however, the AMA was reformulating its code of ethics to allow physicians more flexibility in applying for and receiving patents. The rather severe language of the 1905 Code was replaced, in 1940, by more ambiguous language: "It is unprofessional to receive remuneration from patents or copyrights on surgical instruments, appliances, medicines, foods, methods, or procedures. It is equally unprofessional by ownership or control of patents or copyrights either to retard or to inhibit research or to restrict the benefit of patients or the public . . ." ¹⁴⁹ This revised language suggests that it was acceptable for physician-inventors to patent their inventions, but not to enforce them or receive licensing fees.

In 1952, the patent law was recodified as Title 35 of the U.S. Code and the first level of the filter of patentability was codified as 35 U.S.C. § 101 ("Patentable Subject Matter"): "Whoever invents or discovers any new and useful process, machine, manufacture, or

PAT. OFF. SOC'Y 371; Letter of George Benjamin, at 28 J. PAT. OFF. SOC'Y 842; and Letter of L.A. Austrian, 28 J. PAT. OFF. SOC'Y 844. I.J. Fellner's response to the comments of George Benjamin was also published at 28 J. PAT. OFF. SOC'Y 678 (1946).

145. Fellner, *Therapeutic Methods*, *supra* note 124, at 106-08.

146. Austrian, *supra* note 144, at 844 (emphasis in original).

147. Sperry, *supra* note 27, at 371.

148. 96 F. Supp. 689, 695 (D. Md.) *aff'd*, 193 F.2d 58 (4th Cir. 1951).

149. AMA PRINCIPLES OF MEDICAL ETHICS 8, § 5 (1940) ("Patents and Perquisites"). For a revealing and extensive overview of university patent policies regarding medical patents during the 1930s and 1940s, see PALMER, *supra* note 27 (also providing synopsis of AMA ethical guidelines).

composition of matter, or any new and useful improvement thereof, may obtain a patent" For the first time the patent statute provided for the explicit protection of *processes*. In light of this new language, the PTO overruled *Brinkerhoff* only two years later in *Ex parte Scherer*,¹⁵⁰ which held that a method of jet-injecting fluids under a patient's skin was patentable. With *Scherer*, the Patent Office Board of Appeals thus formally opened the field of medical process patents. The Board effectively reversed *Brinkerhoff's* presumption that medical processes were unpredictable and hence unpatentable, noting that the new patent statute did not "categorically" define medical processes as unpatentable.¹⁵¹

In 1955, only one year after *Scherer*, the AMA again modified its view of the ethics of patenting medical devices. Now it would be ethical for a physician "to patent surgical instruments, appliances, and medicines, or copyright publications, methods, and procedures."¹⁵² Only the uses of or profits from these patents and copyrights that would "retard or inhibit research or restrict the benefits derivable" were deemed unethical.¹⁵³ The AMA condoned physicians' profiting from the enforcement of patent rights, as long as these profits did not "inhibit research" or "restrict benefits."

Recent developments have led to even broader definitions of "patentable subject matter." Hailed by many as the spark that ignited the modern biomedical industry, the Supreme Court's ruling in *Diamond v. Chakrabarty*¹⁵⁴ significantly expanded the scope of patentable subject matter by dismissing a broad range of ethical arguments designed to narrow the range of patentable inventions. In *Chakrabarty*, a narrowly divided Court held a man-made bio-organism patentable and concluded that the relevant distinction under the patent law was "not between living and non-living, but between products of nature . . . and human-made inventions."¹⁵⁵ The Court dismissed the many hazards feared to accompany biomedical science, noting that whether "claims are patentable may determine whether research efforts are accelerated by hope of reward or slowed by want

150. 103 U.S.P.Q. (BNA) 107 (Pat. Off. Bd. App. 1954).

151. *Id.* at 110.

152. AMA PRINCIPLES OF MEDICAL ETHICS 11-12, § 7 (1955) ("Patents and Copyrights"). For a review of the various AMA ethical standards during the 1950s, see Edgerton, *supra* note 6, at 564-67 (concluding that the medical profession generally endorses the use of the patent system as a tool for bringing inventions into general use, provided the invention is made widely available and is exploited with dignity).

153. AMA PRINCIPLES OF MEDICAL ETHICS 11-12, § 7 (1955) ("Patents and Copyrights").

154. 447 U.S. 303 (1980) (Burger, J.) (5-4 decision).

155. *Id.* at 313.

of incentive,"¹⁵⁶ but need not determine the ultimate value of the research to society. Other regulatory agencies, such as the FDA, could better determine the social and medical value of such inventions.¹⁵⁷ The Court intimated that if Congress felt a need to monitor an ethically troubling technology, it could empower an agency to oversee that technology.¹⁵⁸ The same reasoning may be at work in the current Senate bill.¹⁵⁹ That bill would apparently provide that if and when FDA authority expands to govern medical processes, medical process patents would be enforceable against physicians, patients, or other health care entities. However, as long as no federal agency is empowered to regulate the use of medical processes, medical process patents should be, by and large, unenforceable.

The creation of the Court of Appeals for the Federal Circuit (CAFC) in 1982¹⁶⁰ further signaled a strengthening of the patent grant, as it unified the appellate jurisdiction of patent disputes and judicial review of the PTO in a single federal appellate court. The CAFC recently sealed the fate of the "beneficial utility" standard for medical patents. In *In re Brana*, the court (with the PTO's blessing) yielded all authority to regulate the safety and efficacy of medical products to the FDA.¹⁶¹ If and when the scope of federal regulatory authority expands to govern the use of medical processes, *Brana* suggests that the PTO would again yield to a sister agency.

In light of the broad construction of 35 U.S.C. § 101 now favored by the courts, the unified jurisprudence of the CAFC, and the ever-relaxing ethical standards of the AMA, it should come as no surprise that medical process patents have become quite

156. *Id.* at 317.

157. *Id.*

158. *Id.*

159. See *supra* note 8 and accompanying text.

160. The Federal Courts Improvement Act of 1982, Pub. L. 97-164, 96 Stat. 25 (codified, in part, as 28 U.S.C. § 1295(a) (1988)) (including in the jurisdiction of the CAFC appeals from decisions of the PTO Board of Patent Appeals and Interferences and of federal district courts to which a case was directed pursuant to Title 35 of the U.S. Code (The Patent Act)).

161. 51 F.3d 1560, 1567 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995)). See also "<http://www.fda.gov/opacom/hpcdrh.html>" (describing the FDA's Center for Devices and Radiological Health, which is responsible for ensuring the safety and effectiveness of medical devices), "<http://www.fda.gov/opacom/hpdrug.html>" (describing the FDA's Center for Drug Evaluation and Research, which regulates prescription and over-the-counter medicines for human use), and "<http://www.fda.gov/opacom/hpvet.html>" (describing the FDA's Center for Veterinary Medicine, which ensures that animal drugs and medicated feeds are safe and effective), all on the World Wide Web.

commonplace.¹⁶² Nonetheless, in a June 1994 resolution, the AMA condemned physicians who would seek patents for "medical and surgical" procedures,¹⁶³ while it continued to tacitly approve physicians who would patent surgical or diagnostic instruments.¹⁶⁴

In view of the medical community's continually changing views on the ethics of obtaining medical patents,¹⁶⁵ as well as the changing role of the PTO in adjudicating the social and ethical worth of patent applications, the AMA's support of the pending legislation¹⁶⁶ should raise some eyebrows at the very least. In the following part, I advance a scheme better suited to understanding the implications medical patents have for the ethical concerns of patient autonomy and privacy, as well as for physicians' potential conflicts of interest. Using this scheme as a framework, I then propose a mandatory assignment system for physician-inventors, which will address both the concerns of the medical community and the underlying policies of the patent law.

V. A CLASSIFICATION SCHEME FOR ADDRESSING WHETHER MEDICAL PROCESSES SHOULD BE PATENTABLE

The foregoing analysis suggests that the proposed statutory distinctions between medical product claims and medical process claims may be no more than historical accident. However, the historical analysis alone does not address the possibility that serious ethical and practical differences may be reflected in the distinction between medical products and processes sought in the proposed legislation. In this part, I address the ethical and social concerns

162. See Noonan, *Patenting Procedures*, *supra* note 7, at 658-60 (1995) (Table 1, listing 48 selected medical process patents but maintaining that such patents are not a "recent phenomenon"). See also Felsenthal, *supra* note 7, at B1; Neergaard, *supra* note 7, at A14.

163. At Supplemental Resolution 2, A-94 (§ 480.975) (1994) the AMA condemned "the patenting of medical and surgical procedures" and announced its intention to work with Congress to outlaw the patenting of such procedures.

164. AMA CODE OF MEDICAL ETHICS: CURRENT OPINIONS AND ANNOTATIONS 140, § 9.09 (1994) ("Patent for Surgical or Diagnostic Instrument"), which provides: "A physician may patent a surgical or diagnostic instrument he or she has discovered or developed. The laws governing patents are based on the sound doctrine that one is entitled to protect one's discovery."

165. I am aware that the AMA does not represent the entire medical community. I have simply chosen the AMA as a convenient mechanism to trace the evolving views of the medical community.

166. In June of 1995, Dr. John Glasson, Chair of the AMA Council on Ethical and Judicial Affairs, presented the *AMA Report*, *supra* note 10, articulating the AMA's support for H.R. 1127 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

raised by the three broad classes of medical patents and focus on the three chief ethical concerns discussed in part III: autonomy of patients and physicians, patients' rights to privacy, and the maintenance of sound physician-patient relationships. I then conclude that while the two pending bills crudely distinguish among types of medical patents, neither resolves the ethical concerns common to the classes. Rather, a distinction based on whether or not a physician owns the patent would more effectively address the ethical concerns raised by medical patents.

A. Medical Product Claims

The first class of patent claims, those protecting new medical products (and necessarily protecting their use in medical treatments), are typified by claims for synthetic drugs and medical devices.¹⁶⁷ Such innovations are patentable in the U.S.,¹⁶⁸ throughout Europe,¹⁶⁹ and, under the recent General Agreement on Tariffs and Trade, Agreement on Trade Related Aspects of Intellectual Property Rights (GATT-TRIPS) accord, in all World Trade Organization (WTO) countries.¹⁷⁰ It is thus accurate to say that international consensus supports the patentability of medical products.

This consensus seems odd, however, in view of the developing international controversy surrounding the patenting and marketing of pharmaceuticals.¹⁷¹ For example, Glaxo PLC, the world's second largest pharmaceutical producer and owner of a patent for the best-selling prescription medicine Zantac, has recently seen its sales decline as entire countries,¹⁷² as well as several domestic health

167. Medical product claims are often classified by the PTO as belonging to either utility patent class 424 ("organic compounds/medical") or classes 602-604 ("Medical & Surgical Equipment").

168. 35 U.S.C. § 101 (1988) ("any new and useful process, machine, manufacture, or composition of matter" is patentable).

169. EPC Article 52(4). See *supra* note 12.

170. General Agreement on Tariffs and Trade, Agreement on Trade Related Aspects of Intellectual Property Rights (GATT-TRIPS) Article 27 ("Patentable Subject Matter") provides, in part: "[§ 1] [P]atents shall be available for any invention, whether products or processes, in all fields of technology, provided they are new, [are non-obvious] and are capable of an industrial application," subject to the provision that member states may exclude from patentability "[§ 3(a)] diagnostic, therapeutic and surgical methods for the treatment of humans or animals."

171. See, e.g., Stephen D. Moore & Elyse Tanouye, *Innovation Fails to Shield Glaxo in HMO World*, WALL ST. J., Jan. 25, 1995, at B1, B4.

172. *Id.* at B4 ("[T]he French government has refused to pay for patients' use of the [highly-touted migraine] drug, as it is still wrangling with Glaxo over a price, and health authorities in the Netherlands wrested sizable price cuts by threatening to deny coverage for its citizens.").

maintenance organizations (HMOs), have refused to purchase particular pharmaceuticals. These countries and HMOs believe the drug is overpriced and redundant of less expensive options.¹⁷³ While these developments may be seen as mere market corrections for overpriced goods, the fact remains that millions of patients are denied access to such new treatments by the elevated prices often attached to patented pharmaceuticals,¹⁷⁴ as well as by governmental and HMO austerity measures.

Even more severe ethical objections are raised where a patent holder exercises its right to exclude others from the market while not producing the patented medical product itself. Although every medical product claim potentially raises this concern, the courts do consider the potential public harm of enforcing an injunction in favor of such an unscrupulous patentee.¹⁷⁵ For example, in *Milwaukee v. Activated Sludge, Inc.*,¹⁷⁶ the appellate court denied an injunction against the use of a waste treatment system on the theory that enforcement would have created an irreparable harm to the local community.¹⁷⁷ The CAFC has suggested¹⁷⁸ that it will continue to deny injunctions where the patent-holder has simply failed to exploit its

173. *Id.*, at B1, B4.

174. The patent grant gives its owner the right to prevent others from selling the patented product during the patent term. If the patentee can sell the product during that term and no noninfringing substitute is available to consumers, the patentee can elevate the price of the product without fear of direct competition in a narrowly defined market. The potential to capture such a market, in essence, creates the incentives underlying the patent system. For a more detailed analysis of these incentives, see Eisenberg, *Patents, supra* note 63, at 1024-30.

175. 35 U.S.C. § 283 (1988) provides that federal courts have jurisdiction to "grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent, on such terms as the court deems reasonable." The CAFC has justified always considering public benefits and harms when reviewing injunctions by noting that the standards of public interest, not the requirements of private litigation, measure the need for injunctive relief, *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858, 868 (Fed. Cir.), *cert. denied*, 469 U.S. 856, 865-66 (1984), and that "[i]f Congress wants the federal courts to issue injunctions without regard to historic equity principles, it is going to have to say so in explicit and even shameless language," *id.* at 867 (quoting *Hecht Co. v. Boules*, 321 U.S. 321, 331 (1944)). See also *Reebok Int'l v. J. Baker, Inc.*, 32 F.3d 1552, 1555 (Fed. Cir. 1994); *Chrysler Motors Corp. v. Auto Body Panels of Ohio*, 908 F.2d 951, 954 (Fed. Cir. 1990).

176. 69 F.2d 577 (7th Cir.), *cert. denied*, 293 U.S. 576 (1934).

177. *Id.* at 593.

178. In *Kearns v. Chrysler*, 32 F.3d 1541, 1551 (Fed. Cir. 1994), the court cited *Vitamin Technologists v. Wisconsin Alumni Research Foundation*, 146 F.2d 941, 944-45 (9th Cir. 1944) (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose). The court used this citation to support the uncontroversial proposition that "the right to exclude . . . is not absolute even during the life of a patent, but is discretionary." *Kearns*, 32 F.3d at 1551.

patent rights,¹⁷⁹ or when an injunction would deny the public access to necessary medical products.¹⁸⁰ Nevertheless, the owner of a vital medical product patent may lawfully extract monopoly prices during the term of the patent and thus can create severe barriers to most patients' access to health care.

The enforcement of surgical device patents, covering either devices used during surgery or those left in the body of the patient, may also infringe upon patients' rights to privacy.¹⁸¹ Where a claim protects a device, a patent owner need only "mark" the device with the U.S. patent number to assure the recovery of damages¹⁸² from anyone who "uses or sells" the device without the permission of the patent owner.¹⁸³ In *American Medical Systems, Inc. v. Medical Engineering Corp.*, the CAFC justified this rule in the context of claims covering an implanted medical device and a method of implanting the device.¹⁸⁴ The court's ruling suggests that both physicians (by using or selling medical devices) and patients (by using medical devices) may be liable for damages, even where an implanted, hence unseen, device is used. To enforce such claims, a patentee (or, perhaps, a court) may be forced to inspect whether an appropriate "mark" was affixed to the implanted device, potentially encroaching upon patients' rights to privacy during and after surgery.

Agreements between physicians and pharmaceutical or medical device companies may also lead to severe conflicts between the financial interests of the physician and those of the patient. For example, if a physician were compensated by a patentee for

179. *E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 835 F.2d 277 (Fed. Cir. 1987) (denying injunction).

180. *Vitamin Technologists*, 146 F.2d at 945 (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose).

181. *Annas*, *supra* note 7, at 25.

182. 35 U.S.C. § 287(a) (1988). *See also* *American Medical Sys. v. Medical Eng'g Corp.*, 6 F.3d 1523, 1538 (Fed. Cir. 1993), holding:

The purpose behind the marking statute is to encourage the patentee to give notice to the public of the patent. The reason that the marking statute does not apply to the method claims is that, ordinarily, where the patent claims are directed to only a method or process there is nothing to mark. Where the patent contains both apparatus and method claims, however, to the extent that there is a tangible item to mark [the patent holder must affix a mark to] avail itself of the constructive notice provisions of section 287(a).

183. 35 U.S.C. § 271(a) (1988).

184. *American Medical Sys.*, 6 F.3d at 1538-39 (holding claims for an inflatable, prosthetic penile implant and for a method for implanting the device were infringed willfully, but where no notice of a valid U.S. patent appeared on the device, district court correctly denied damages).

prescribing a patented medication, the physician would have strong financial interests potentially adverse to the interests of the patient. Only in extreme cases does medical malpractice liability provide incentives counter to the positive incentives for financial agreements between physicians and pharmaceutical companies. Where several courses of treatment are available, the potential for abuse and conflicts of interest should be self-evident. In fact, the regulation of agreements between pharmaceutical manufacturers and physicians is currently the subject of intense debate,¹⁸⁵ indicating that the more narrow concerns raised by medical product patents are real.

In light of these strong ethical and conflict-of-interest concerns, the consensus of support for medical product patents may seem odd. However, when the high costs of developing new and more effective pharmaceuticals and the strong regulatory role entrusted to the FDA are considered,¹⁸⁶ rationales for protecting medical product claims do emerge. The investments needed for research expenditures justify patent protection; and, because most product patent owners are not physicians and may be prevented from influencing physicians, situations that give rise to conflicts of interest may be avoided through appropriate regulation. These considerations soften the ethical and conflict-of-interest concerns of medical product patents, if only slightly.

B. Medical "New Use" Claims

The second class of patent claims, those protecting new medical uses for known products, presents a distinct set of ethical dilemmas because the product is "available" but the use valued by physicians and their patents is protected by a distinct claim. This class of claims is typified by any newly discovered medical applications of a known technology,¹⁸⁷ such as the use of a laser in arterial surgery¹⁸⁸ or the use of a hair loss treatment to combat a reproductive disorder.¹⁸⁹

185. RODWIN, *supra* note 2, at 55-94.

186. The FDA is empowered to regulate pharmaceuticals for human or animal use, medicinal feeds for animals, and medical devices. For more information, see generally "<http://www.fda.gov>" on the World Wide Web.

187. Medical "new use" claims, like medical product claims, are often classified by the PTO as belonging to either class 424 ("organic compounds/medical") or classes 602-604 ("Medical & Surgical Equipment").

188. See U.S. Patent No. 4,862,886 (1989) ("Laser Angioplasty"). Assignee Summit Technologies owns eight patents related to the use of lasers in medical treatments. While some of these patents are, strictly speaking, medical process patents, many contain specific "new use" claims for the purposes of this analysis.

189. See U.S. Patent No. 5,336,678 (1994) ("Use of Minoxidil for Treating Erectile Impotence").

Under the House bill these claims would not be allowable unless the underlying technology, be it a device or a pharmaceutical, is independently patentable.¹⁹⁰ However, under the Senate bill these claims would be allowable and could be enforced against physicians if the "known" technology were a drug or device subject to either the Food, Drug and Cosmetics Act or the Public Health Service Act.¹⁹¹ The House bill would effectively eliminate medical "new use" claims, while allowing owners of product patents, alone, to license *all* uses of their product, even those uses developed by others.¹⁹²

This proposed elimination of medical "new use" claims is startling, because the strong ethical objections raised against medical product patents are often tempered by the existence of other patents containing "new use" claims. In the context of a "new use" patent "blocked" by an earlier product patent, *neither* patent owner may lawfully practice the invention without a license from the other. In such a situation, both patentees must compromise to bring the product to market and, often, artificially elevated prices cannot be maintained because both patentees ultimately enter the market.¹⁹³ Where no "new use" claims may be granted, the original patentee may forbid any use of the product and may extract monopoly prices for whatever new medical uses it, or others, develops. This perverse situation creates strong *disincentives* for the development (and disclosure) of new medical uses of a patented product by anyone other than the original patentee, since all financial benefits derived from the new use would return to the original patentee instead of being shared by both inventors.¹⁹⁴

Despite this odd consequence, the elimination of "new use" claims does alleviate certain ethical objections, especially the objection that "new use" claims potentially inhibit physicians' autonomy. Traditionally, physicians have had broad authority to prescribe any FDA-approved pharmaceutical for any ailment, even if

190. See H.R. 1127, *supra* note 8.

191. See S. 1334, *supra* note 8.

192. *Hearings, supra* note 31 (testimony of Dr. Frank Baldino, Jr., President and Chief Executive Office of Cephalon, Inc.). Dr. Baldino testified that "despite the voiced intention of only focusing on pure medical procedure patents, H.R. 1127 would prevent the issuance of precisely the types of patents [new use patents] which Cephalon and members of our industry must secure in order to protect our discoveries."

193. MERGES, PATENT LAW, *supra* note 1, at 182-86.

194. Admittedly, the term of the original product patent and that of the "new use" patent may overlap for only a few years. In such a situation, the "new use" would enter the public domain more rapidly under H.R. 1127 than it does under the present system, but the strong disincentives for anyone but the patentee developing a medical "new use" during the term of the product patent would still remain.

the compound is not suggested for the prescribed use. "New use" claims, if enforced, would limit a physician's ability to prescribe useful drugs as freely as the traditional principles of physician autonomy suggest.

The elimination of "new use" claims might also allay some concerns regarding physicians' conflicts of interest. Physician-inventors with patent rights for new medical uses might encourage other physicians to use or license these uses, even though cheaper or more effective treatments are available. By eliminating "new use" claims, the House bill removes this potential conflict of interest in much the same way it eliminates the potential conflicts that arise from medical product claims. However, even if the elimination of "new use" claims would allay present concerns over physicians' autonomy and potential conflicts of interest, it would do so while creating a perverse incentive against developing new medical uses for already patented products and a concurrent incentive to conceal all such developments during the term of the dominant product patent. With regard to "new use" patents, then, the Senate bill may be a viable alternative since it would retain "new use" patents and leave the vast majority of such patents enforceable.

C. "Pure" Medical Process Claims

The third and final class of medical claims, those protecting only manipulative steps such as surgical procedures, would be unpatentable under the House bill and unenforceable under the Senate bill.¹⁹⁵ The patenting of medical and surgical techniques triggers concerns over both the "sharing norm" in the medical community and the invasion of patients' rights to privacy. However, the specter of physician-inventors enforcing their patent rights by sending investigators into operating rooms to oversee potentially infringing procedures most directly triggers concern only over patients' rights to privacy.¹⁹⁶

The mechanics of enforcing patent rights is also important in that it blurs the distinction between the scope of patent protection available under the European Patent Convention (EPC), Article 52, and that available under the proposed legislation. The EPC makes all medical processes unpatentable, but it allows for the patenting of medical devices.¹⁹⁷ The House bill is distinguishable in that it would allow for a patent covering a medical process, provided that an

195. S. 1334, *supra* note 8.

196. Annas, *supra* note 7, at 25-26.

197. EPC Art. 52 ("Patentable Inventions"), ¶ 4. See *supra* note 12.

independently patentable device is "necessary" to the process."¹⁹⁸ In the context of enforcement (where the real-world value of the patent right is determined), this subtle distinction becomes irrelevant. Enforcement of patent rights will rely on detection of the underlying device under either regime. Under the House bill, the process patent could not exist, and would therefore have no value, without the claim covering the "necessary" device. Thus, the narrow exception of the House bill becomes all but meaningless.

The Senate bill takes a different approach. Under it, most "pure" medical or surgical processes would be patentable but would not be enforceable. To differentiate between patents protecting "pure" processes and the two other types of medical patents, the bill relies on the limited regulatory authority of the FDA.¹⁹⁹ As noted above, the FDA has the authority to regulate medical devices and pharmaceuticals but no direct authority to regulate medical or surgical procedures. Because procedure patents (unlike the two other types of medical patents) are not the subject of federal regulation, only patents for "pure" medical procedures would be unenforceable under the Senate bill.

Nevertheless, both bills address some of the potential conflicts of interests that may arise for physicians who own patent rights for new processes. Incentives presently exist, and would still exist under the narrow exception of the House bill, for a physician-inventor to recommend to other physicians, as well as to his patients, that they practice his patented surgeries. These conflicts are especially acute because of physicians' special roles as medical advisors. Relatively free of FDA regulation when prescribing "pure" surgical or diagnostic procedures, physicians (especially surgeons) are entrusted with critical surgical decisions by many patients, even though they are also the very individuals who patent, and profit from, these recommended surgical procedures.

The Senate bill addresses this conflict by tying enforceability to the scope of FDA regulatory authority. But concerns about patients' rights to privacy and physicians' conflicts of interest would not disappear if the FDA (or another federal agency) were given the authority to regulate medical or surgical procedures. Furthermore, the Senate bill fails to address the many ethical concerns raised by physician-owned patents other than the narrow class of "pure" process patents.²⁰⁰ The bill may also create an artificial reason to limit the

198. H.R. 1127, *supra* note 8.

199. S. 1334, *supra* note 8.

200. See generally Noonan, *Patenting Procedures*, *supra* note 7.

scope of FDA authority so that medical process patents would be enforced. Therefore, although the Senate bill may be a superior alternative since it addresses a concern the House bill does not, it fails to identify the only truly relevant distinction among the three types of medical patents.

D. The Relevant Distinction: The Inventor's Identity

The foregoing analysis of the three classes of medical patent claims indicates that, from the narrow perspective of medical ethics, the classes are not distinguishable in any meaningful way. While medical "new use" and process claims may lead to conflicts of interest more difficult to regulate than those of medical product claims, medical product claims present stark ethical dilemmas by restricting physician autonomy, patient autonomy, and access to health care. Also, medical product claims, if strictly enforced, threaten patients' rights to privacy far more severely than either "new use" or process claims.

The PTO and the courts might also find it difficult to distinguish "mere" medical process claims from otherwise patentable claims under the House bill and, likewise, to determine the precise scope of FDA authority under the Senate bill. The courts that interpret the EPC (where therapeutic methods are not patentable but industrial applications are)²⁰¹ have struggled with this distinction. These struggles should caution against the use of rules that draw facile distinctions between "medical" innovations, which are to be freely shared, and "industrial" innovations, which might be kept secret if not for the prospect of patent protection. The European Patent Organization's Technical Board of Appeal, in *In re Bayer AG*,²⁰² was forced to decide if the addition of a particularly effective immunostimulant to poultry feed for boosting market weight was an unpatentable "method of treatment of the animal body" or a patentable process "susceptible to industrial application." The Board based its holding of unpatentability on rather opaque reasoning: (1) the medical aspects of the process were "inextricably linked to" rather than "distinct from" the cosmetic aspects,²⁰³ (2) the process was "curative" rather than "prophylactic,"²⁰⁴ and (3) increased market

201. EPC Art. 52 ("Patentable Inventions"), ¶ 4. See *supra* note 12.

202. Decision of the Technical Board of Appeal 3.3.2, T780/89 (Aug. 12, 1991), OJ EPO 7/1993, 440. It is unclear whether H.R. 1127 includes veterinary medicine in its definition of "medical." The EPC, however, clearly treats animal and human medical processes alike.

203. *Id.* § V, ¶¶ 3.1, 3.2, 3.3.

204. *Id.* § V, ¶ 3.5.

weight was not an "industrial application" but "merely a consequence of the therapeutic treatment."²⁰⁵ Clearly, in this and a number of other situations,²⁰⁶ the distinctions between industrial and medical (that is, between advances which require the incentive of patent protection and those that do not) may be difficult to justify or even explain.

The logical question, then, is by what other criteria may the patents that raise ethical objections be distinguished from the patents that do not? Or, more appropriately phrased: What else about medical process claims makes them the target of the medical community and the proposed legislation? The arguments that product and "new use" inventions are often more costly to develop or are more "tangible" in a way that merits protection²⁰⁷ are often inaccurate and hence, as *In re Bayer AG* demonstrates, difficult to rationalize.

Perhaps the distinction lies not so much in the claimed subject matter, but in the professional role of the inventor. Physicians, logically enough, are most often the inventors of medical processes and "new uses," but rarely develop new pharmaceuticals or devices.²⁰⁸ Thus, even though they are rarely expert synthetic chemists or mechanics, physicians are in a unique position to "experiment" with novel uses for known technologies and explore new surgical and therapeutic processes. In this regard, it is interesting to note that before what may be termed the "compartmentalization" of medicine (with synthetic chemists or mechanics working alone on their inventions, far from the hospital), physician-inventors were more closely involved in the development of all medical technologies.²⁰⁹ Perhaps, then, it is not mere coincidence that the AMA's long-forgotten prohibitions against the patenting of any medical innovation were in force during the time when physicians typically invented all types of medical patents. I suggest that as the role of physician-inventors in developing medical products disappeared, the

205. *Id.* § V, ¶ 7.

206. See *Hearings, supra* note 31 (testimony of Dr. William D. Noonan). Dr. Noonan testified that "European patent practice allows a new use of a known drug to be patented as a 'composition for use in the treatment' of a pathological condition" in spite of the ban against patents protecting methods of treating the human or animal body.

207. In fact, proponents of the House bill have made this argument. *Hearings, supra* note 31 (testimony of Dr. H. Dunbar Hoskins, Jr. and Dr. Jack A. Singer).

208. *Hearings, supra* note 31 (testimony of Dr. Charles D. Kelman). Dr. Kelman testified that "the advancements [in medical procedures] occur through gradual, on-the-job improvements and refinements of known methods in operating rooms and physicians' offices."

209. See PALMER, *supra* note 27 (providing a thorough analysis of medical patent policies for the first three decades of the twentieth century).

prohibitions against such patents became far less severe. Now that practicing physicians rarely develop medical products on their own, objections to the patenting of medical products are rarely voiced.²¹⁰

This modern reality coupled with the lack of important differences between "objectionable" and "non-objectionable" medical patents leads to the conclusion that the only relevant distinction, with respect to ethical or conflict-of-interest concerns, lies in who owns (and is therefore empowered to enforce) the patent rights. The most serious ethical objections are raised only where physician-inventors own, license and attempt to enforce their own medical patents, or where physicians have interdependent relationships with other medical patent owners.

Very often, however, physician-inventors must assign all of their patent rights to the institutions for which they work and do not play an active role in the licensing or enforcement of the patent. At university medical centers this was an accepted, if rare, practice until passage of the Bayh-Dole Act in 1980.²¹¹ After that legislation allowed patents to issue for the inventions developed with the aid of federal grants, nearly all major university medical centers created technology transfer administrations.²¹² These administrations have served a valuable role by creating incentives to pursue both basic and applied research, reducing the costs of individual licensing transactions, and fostering cooperation between academia and industry.²¹³ Unlike individual inventors, technology transfer administrations have strong incentives, both internal and external, to share medical technology. Because relatively large organizations

210. See *supra* part V.A.

211. Pub. L. No. 96-517, 94 Stat. 3019 (1980) (codified as 35 U.S.C. §§ 200-212 (1988)) ("Chapter 18. Patent Rights in the Inventions Made with Federal Assistance").

212. GARY W. MATKIN, AMERICAN COUNCIL ON EDUCATION, TECHNOLOGY TRANSFER AND THE UNIVERSITY (1990) (citing Gary W. Matkin, Technology Transfer and the American Research University (1989) (unpublished Ph.D. dissertation, University of California (Berkeley))). See generally Reid G. Adler, *Technology Transfer, Government Research, and the Frontiers of Science: Intellectual Property Protection in the Biotechnology Industry*, 39 FED. BAR NEWS & J. 270 (1992); Brian J. Reichel, *Regulating Conflicts of Interest in the Technology Transfer Age: Promoting Public Trust Or Defeating Public Interest?*, 40 DRAKE L. REV. 385, 398-402 (1991) (summarizing the history of private, public and federal technology transfer administrations).

213. See 60 Fed. Reg. 12,771 (1995) (National Institutes of Health's (NIH) Uniform Biological Materials Agreement (UBMTA)). See also Richard Stone, . . . *While NIH Unveils a Tech Transfer Treaty*, 268 SCIENCE 19 (1995) (discussing the NIH-UBMTA and claiming it will speed the transfer of proprietary materials); Arthur George et al., *The Commercial Campus*, THE RECORDER (SAN FRANCISCO, CA), INTELLECTUAL PROPERTY SUPPLEMENT, Mar. 6, 1995, at 38 (discussing evolving role of university technology transfer administrations) (on file with author).

must constantly license "in" a variety of patented technologies for their own members to use, they are far less likely to refuse to license "out" any single patented technology than an independent physician-inventor with a narrow specialty would be.²¹⁴ Also, institutional technology transfer administrators are subject to the scrutiny of academic researchers, who may value and enforce the "sharing norm."²¹⁵ For these reasons, and because institutional technology transfer may be a more efficient means of recovering the costs of research and development than independent inventors licensing their own patent rights, nearly all major research centers now have some form of technology transfer administration.²¹⁶

VI. A PROPOSAL: MANDATORY ASSIGNMENT OF PHYSICIANS' PATENT RIGHTS

The central dilemmas facing independent physician-inventors, then, are that the patent system provides incentives for them to disregard the "sharing norm" of medical science and to overlook their ethical and fiduciary duties to patients. The "sharing norm" and the concerns raised by breaches of a fiduciary duty do not confront the inventors of most medical products because "sharing" is no longer a strong ethical norm in the industries most often involved with the development of pharmaceuticals or medical devices. Likewise, these inventors owe no meaningful fiduciary duty to individual patients. The enforcement of patent rights may also lead physicians to disregard their ethical obligations to preserve patients' privacy and autonomy.

The pending legislation and the current AMA Principles of Medical Ethics tacitly recognize that only non-physicians are responsible for the development of medical products, by admitting that patenting such inventions is ethical and in fact should be encouraged. In seeking to impose a "sharing norm" on *only* physician-inventors, the medical community has overreacted, attempting either to outlaw all the patents physician-inventors would typically own or to prevent the enforcement of their patent rights. In so doing, the medical community has overlooked a far less drastic alternative: entrusting the enforcement of the "sharing norm" and the associated ethical and fiduciary duties to organizations subject to the oversight of the medical community.

214. I am not aware of any empirical evidence that supports this assertion, but I suggest the underlying logic is compelling.

215. See *supra* part II.A.

216. MATKIN, *supra* note 212. See also Adler, *supra* note 212, at 270.

In June of 1914, the House of Delegates of the AMA gave permission to the association's Board of Trustees "to accept, at their discretion, patents for medical and surgical instruments and appliances and to keep these patents as trustees for the benefit of the profession and the public; provided neither the [AMA] nor the patentee shall receive remuneration from these patents."²¹⁷ At that time few (or no) medical process patents were issued by the PTO, and the AMA strongly disapproved physician-owned patents of any kind. Nevertheless, the AMA could have held itself out as a repository for medical patents developed by concerned non-members. It appears that too few of these generous inventors stepped forward and that even fewer physicians were willing to offer evidence that they had violated the AMA's ethical code. Thus, the AMA never became the national medical patent clearinghouse the House of Delegates may have envisioned.

A. Patent Clearinghouses for Physician-Invented Patents

I have argued that the current debate over the patentability of medical processes and the ethical and conflict-of-interest objections raised by these patents are, by and large, merely objections to the ownership and enforcement of patents by practicing physicians.²¹⁸ A mandatory assignment system limited to physician-inventors, therefore, could resolve much of the current debate. Such a mandatory assignment system, in which incentives to invent coexisted with safeguards against the violation of ethical norms, can be easily envisioned.

Organizations subject to the governance of a significant portion of the medical community (much like the AMA) could manage patent clearinghouses for the rights of otherwise independent physician-inventors. To ensure that all physicians participated in a clearinghouse, each organization would have to be approved by various state medical licensing boards. Furthermore, as a requirement to licensure, every physician would be required to assign any patent rights to one of the several state-approved clearinghouses. A university-affiliated physician would have the option of assigning her patent rights to the university, if it had been approved by the state.

Certain uniform rules would apply to all of the clearinghouses. Each would be required to offer all of its rights as a package to

217. Fishbein, *supra* note 6, at 1317 (discussing proposal of 1914). Also described in Sperry, *supra* note 27, at 372 and in PALMER, *supra* note 27.

218. See *supra* part V.D.

medical centers throughout the country. While each could employ different formulas to determine licensing rates, those rates would reflect only the size, location, or specialty of a potential licensee medical center, *not* the number of times a specific invention has been used by that hospital in the past. Meanwhile, member physician-inventors would be reimbursed on a per-use basis, and only medical records containing no identifiable information about individual patients (e.g., physicians' medical malpractice insurance records or hospitals' operating room logs) would be used to confirm the number of times a specific product or process was used. In this way, the invasions of patients' rights to privacy that most often result from enforcement of a patent could be avoided.²¹⁹

However, the details of each clearinghouse's licensing and enforcement scheme could be left to the individual organizations. For example, universities likely would simply retain their present technology transfer offices, but other organizations could look to their membership to strike an appropriate balance between profits and generosity. This variety would allow each physician to select an appropriate clearinghouse for his particular needs and desires. For example, if a physician wishes to license any future invention freely, he would select an appropriate clearinghouse. If, however, he wishes to recover research costs through patent rights, he could choose a clearinghouse with an appropriate licensing structure. Thus, by modeling their activities on existing technology transfer administrations, the proposed patent clearinghouses could become players in a dynamic market.

This proposal finds support in the basic fact that the PTO, when judging the patentability of an invention, is no longer inclined or empowered to enforce society's (much less a given profession's) ethical norms.²²⁰ At the administrative level, such determinations are now

219. Comment, *Medical Process Patents and Patient Privacy Rights*, 14 J. COMPUTER. & INFO. L. 131, 147 (1995) (noting that Montana and Washington have recently enacted modified versions of the 1985 Uniform Health-Care Information Act to protect the confidentiality of medical records). See also MONT. CODE ANN. §§ 50-16-501 to 553 (1987) (Uniform Health Care Information); WASH. REV. CODE ANN. §§ 70.02.005-904 (West 1991) (Medical Records-Health Care Information Access and Disclosure).

220. Merges, *Controversial Technologies*, *supra* note 90, at 1062-68 (concluding that patent protection for a new technology "normally should not be denied on the basis of speculation about potential negative consequences" and that other agencies such as the FDA are better suited to evaluate the potential deleterious effects of new medical technologies). For a more current analysis of the appropriate roles of the PTO and FDA, see *In re Brana*, 51 F.3d 1560, 1564 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995)).

often left to the FDA,²²¹ an agency not answerable to the medical community. The direct control exercised by the medical community over the patent clearinghouses, however, should make the proposed system far more attractive to physicians than either the present system or the proposed legislation's inelegant barriers to the patenting of "pure" medical processes. Additionally, under the proposed system the AMA would play an active role in promoting and assessing new medical technologies. Under both the present system and that of H.R. 1127, the AMA plays no such role.

At yet another level, the proposal creates an enforcement mechanism for the medical community's ethical stance on medical patents. Because boards composed of members of both the medical and research communities could determine rates of compensation for physician-inventors, a physician-inventor's licensing profits need never be so great as to "retard or inhibit research or restrict [social] benefits."²²² The rates at each clearinghouse could be set to strike an appropriate balance among three competing parameters: (1) physician-inventors' desire to recover costs of research and development, (2) physician-inventors' desire to profit from their inventions by extracting a portion of the savings their inventions have afforded society, and (3) the "local" community's desire to provide medical services at the lowest possible cost while still spurring inventions that lead to greater cost savings. The third factor may be seen as a means by which the patent clearinghouse could promote the development of technologies needed to serve society's most basic medical needs by encouraging the development of cost-saving technologies while discouraging the development of certain cost-intensive technologies.

Applying this three-factor rate-setting analysis to the controversial case of Dr. Samuel Pallin,²²³ his clearinghouse might have considered: (1) that Pallin expended virtually no resources in developing his patented incision; (2) that Pallin justifiably desires to extract some of the \$17 his procedure saves each patient; and (3) that there are societal and economic values in reducing the cost of cataract surgery. Balancing these interests in a meaningful way, the clearinghouse could arrive at a reasonable fee at which to reimburse Pallin each time his operation is performed. Such a fee (set, for example, at \$1) would be multiplied by the number of times Pallin's incision is performed over the course of a year (100,000), netting Dr.

221. See *supra* part IV.

222. AMA PRINCIPLES OF MEDICAL ETHICS, 11-12, § 7 (1955) ("Patents and Copyrights").

223. See *supra* part II.

Pallin a handsome reward (nearly \$2 million) during the term of his patent.

Of course, the proposed collection of patent clearinghouses would not resolve all of the ethical and conflict-of-interest concerns raised by medical patents. Pharmaceutical and medical device manufacturers, with justifiable interests in recovering large investments, are often forced to price the latest innovations beyond the financial reach of many patients. Likewise, physicians' conflicts of interest are only partially allayed by the proposed system. While many perverse incentives created by physician-owned patents are eliminated under the proposed system, ties between physician and other holders of medical patents will still raise considerable concerns. The proposal, nonetheless, accomplishes its goal. It reconciles the medical community's need to enforce ethical and professional norms on its members while preserving many incentives to invent and disclose new and more effective medical technologies.

B. ASCAP as a Model for the Patent Clearinghouses

The reader may have already observed that the proposed medical patent clearinghouses closely resemble current copyright clearinghouses, such as the American Society of Composers, Authors, and Publishers (ASCAP) and Broadcast Music, Inc. (BMI). The ASCAP model,²²⁴ a more appropriate model for the proposed patent clearinghouse system, offers four distinct benefits aside from allowing the medical community to enforce its own ethical and professional norms. The proposed system, if closely modeled on ASCAP, will provide for the selling of "blanket" licenses (so called because a single license covers an entire portfolio of rights) to physicians and medical centers. The cost of these licenses would be based only on a medical center's size, specialty, or location. Such a pricing structure would better protect the privacy of patients, for there would be no need to inspect licensee operating rooms for potential infringements. Just as ASCAP uses radio station play lists to calculate only correct disbursements to its members, the medical patent clearinghouses would collect anonymous operating room or laboratory reports to

224. ASCAP represents more than 40,000 members and controls a repertoire of approximately 3 million compositions. Composers, authors and publishers who are members of ASCAP assign their copyrights to the organization in exchange for perpetual royalties, ASCAP's licensing and enforcement services, and representation in ASCAP's governance. For a brief description of ASCAP, its competitor BMI, and their respective methods of operation, see Janet L. Avery, *The Struggle Over Performing Rights To Music: BMI and ASCAP vs. Cable Television*, 14 HASTINGS COMM. & ENT. L.J. 47, 51-53 (1991).

calculate disbursements to physician-inventors. This efficient means of calculating royalties and enforcing patients' privacy rights could compensate inventors such as Dr. Pallin for the correct number of times his procedure was used, while not requiring that hospitals be secretly monitored.²²⁵

A secondary, but compelling, benefit lies in the patent clearinghouse's ability to reduce transactional costs and, in so doing, potentially reduce the cost of medical care in general. All of the individualized licensing, disbursement and enforcement costs that would discourage an otherwise capable physician-inventor from pursuing a new technology would virtually disappear under the proposed system. This physician-inventor, no longer concerned by the costs or stigma of enforcement and assured an equitable return for successful innovative efforts, could focus on developing new, less-costly medical procedures. Additionally, the removal of independent patent holders from licensing negotiations would reduce the number of "hold-outs" who refuse to license technology for a reasonable fee, while eliminating many of the costs of repetitive negotiations.

These latter two additional benefits of the ASCAP model, though more subtle, are no less important. At least part of ASCAP's appeal to its members lies in the organization's willingness to take care of the more "distasteful" business aspects of artists' lives. As far as many members are concerned, if ASCAP affords them suitable royalties while also negotiating licenses, monitoring users, and policing their rights, that is all the better. Similarly, physician-inventors, freed of the more mundane concerns of managing their patent rights, could concentrate more fully on their craft: healing the sick.

A fourth benefit of the ASCAP model is inextricably tied to the other three. One of ASCAP's principal attractions to its members is its representative form of governance. The presence of a representative board of directors, to set both fees and policy, helps guarantee equitable distribution of the proceeds of the licensing agreements while reassuring all members that they have a voice in the organization. Physician-members of the central patent clearinghouse would also benefit from such a system of governance.

225. Of course, "spot checks" limited to verifying operating room logs might be required in exceptional circumstances. Nevertheless, an individual hospital would have no incentive to falsify its logs because the blanket licensing fee would be set independently of uses; it would be based only on the size, location, or specialty of the hospital.

VII. CONCLUSION

The current debate over the propriety of allowing medical process patents, which has worked its way into the U.S. Congress, has provided both the medical and patent law communities an opportunity to examine their current policies. While both communities' policies may be directed toward the same goal, that of providing patients the best and most advanced care at the lowest possible cost, each community pursues distinct, often conflicting, means to that end. The patent system presents powerful incentives to invent and disclose new and useful medical technologies, but it fails to adequately address concerns regarding physicians' adherence to their own code of ethics and their respect for the fiduciary duties owed their patients. This failure indicates that a complete "sacrifice" of medical technologies to the principles underlying the patent law would be unwise.²²⁶ Just as the enforcement of injunctions to enforce patent-holders' rights is always subject to the dictates of public policy,²²⁷ the degree to which patent rights are vested in physician-inventors should be monitored with an eye on the concerns of medical ethics and on the avoidance of conflicts of interest. To the extent that the present patent system provides incentives for physicians to disregard their own professional code of ethics and to breach the fiduciary duties owed their patients, that system should be modified.

At the same time, the medical community values its own ethical and professional standards but disregards the long-term benefits of the patent system. By undervaluing the incentives created by medical process patents, the AMA does a disservice to physician-inventors and to society in general. By completely eliminating medical process patents, the proposed legislation would create perverse incentives for physicians to conceal their discoveries and to abandon promising, though unconventional, new treatments. The proposed legislation would introduce these harms but would address only a few of the ethical and conflict-of-interest concerns raised by medical patents.

The proposal I advance is not entirely novel,²²⁸ but it does provide a viable solution to the impasse between current views in the medical community and the justifications of the patent system. It

226. For a related analysis, suggesting that patent policy should be adapted to the special concerns raised by medical innovation, see Evan Ackiron, Note, *Patents for Critical Pharmaceuticals: The AZT Case*, 17 AM. J.L. & MED. 145 (1991).

227. *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858 (Fed. Cir.), cert. denied, 469 U.S. 856 (1984).

228. Fishbein, *supra* note 6, at 1317. Also described in Sperry, *supra* note 27, at 372 and in PALMER, *supra* note 27.

modifies the present patent system by shifting the burden of distributing and enforcing physician-invented technologies from independent physicians to institutions better suited to that task. It also vests the power to enforce norms of medical ethics and professionalism in organizations answerable to their members, the medical community. Moreover, the proposal represents a meaningful compromise between the positions of the medical community and the strongest proponents of the patent system by placing an efficient enforcement mechanism at the disposal of the medical community. This modified enforcement structure would also safeguard the privacy concerns of patients. Thus, while the proposal does preserve many of the patent system's desirable incentives to invent, it also recognizes the role the medical community must play in enforcing the ethical norms of the profession.

COMMENT

A BEHAVIOR-BASED MODEL FOR DETERMINING SOFTWARE COPYRIGHT INFRINGEMENT

DENNIS M. CARLETON †

TABLE OF CONTENTS

I.	INTRODUCTION	405
II.	DEFINING COMPUTER PROGRAM BEHAVIOR	408
III.	FITTING COMPUTER PROGRAMS WITHIN TRADITIONAL COPYRIGHT LAW	409
	A. Behavior Is Expression	409
	B. Why Behavior Is Protectable	411
	C. Limitations On Protection Of Behavior	416
	D. Computer Programs As Useful Articles	418
IV.	RELEVANT CASE LAW	420
V.	THE PROPOSED BEHAVIOR-BASED TEST	425
VI.	AN APPLICATION OF THE PROPOSED BEHAVIOR-BASED TEST	430
VII.	CONCLUSION	432

I. INTRODUCTION

In 1980, Congress amended the Copyright Act to explicitly recognize copyright protection for computer programs.¹ However, Congress left the task of determining the proper scope of such protection

© Dennis M. Carleton.

† J.D. Candidate, 1996, University of Pittsburgh School of Law; 1983, Master of Software Engineering, Carnegie-Mellon University; 1990, BSEE, Carnegie-Mellon University. The author has ten years of professional software engineering experience. Special thanks to Professor Pamela Samuelson of the University of Pittsburgh School of Law for her comments and help.

1. Pub. L. No. 96-517 § 10(a) (1980) U.S.C.A.A.N. 94 Stat. 3028. The 1980 amendments changed the Copyright Act by adding a definition of "computer program" to section 101, and by adding section 117, which grants certain rights to users of computer programs.

to the courts, providing only that the courts maintain the traditional distinction between idea and expression.²

Since then, courts have grappled with copyright protection for computer programs with mixed results.³ The primary struggle surrounds the extent of copyright protection for "non-literal" aspects of computer programs.⁴ This article suggests that program behavior⁵ must be protected as a non-literal aspect of the program. Furthermore, any test for copyright infringement, absent readily provable literal copying of the programmer's source code, should look solely to the behavioral aspects of the program to determine whether infringement has occurred, eschewing any analysis that dissects a program's structure, organization and other elements related to the programming code.

There are several reasons for advocating this "black box"⁶ type of analysis. First, computer programs are included under the Copyright Act as literary works. As such, they should receive the same level of protection that is extended to other literary works. Thus, the traditional copyright principles and doctrines which protect the non-literal aspects of other literary works should also protect the non-literal aspects of the programmer's expression. Second, the underlying purpose of the Copyright Act supports the protection of program behavior. The behavior of a program is the only aspect of the programmer's expression that is perceived and valued by users. Unless the programmer receives protection from copying of program behavior, the programmer's incentive for producing creative works will be diminished. Finally, there are many ways to write and structure a program so that it will behave in a particular way. As a result, any test for non-literal infringement limited to dissecting the programming code, organization and structure will fail

2. *Id.* The 1980 amendments to the Copyright Act adopted almost verbatim the recommendations of the NATIONAL COMMISSION OF NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT (1979) [hereinafter CONTU REPORT]. The report called for the courts to determine the protectible elements of software. CONTU REPORT, 18.

3. See Irwin R. Gross, *A New Framework For Software Protection: Distinguishing Between Interactive And Non-Interactive Aspects Of Computer Programs*, 20 RUTGERS COMPUTER & TECH. L. J. 107, 132 n.113 (1994).

4. Non-literal aspects of computer programs are "those aspects that are not reduced to written code." *Computer Assoc. v. Altai Inc.*, 982 F.2d 693, 696 (2d Cir. 1992).

5. For a discussion of the definition of the behavior of a computer program, see *infra* part II.

6. The term "black box," as used in computer science, describes the method of software testing whereby the functional interface of the software is tested without knowledge of or regard for the internal implementation of the functions of the program. Compare ROGER S. PRESSMAN, *SOFTWARE ENGINEERING: A PRACTITIONER'S APPROACH* 470, 484 (2nd ed. 1987) and RICHARD E. FAIRLEY, *SOFTWARE ENGINEERING CONCEPTS* 284 (1985) with Duncan M. Davidson, *Common Law, Uncommon Software*, 47 U. PITT. L. REV. 1037, 1080 (1986) (using the term "black box" in a slightly different context to support the notion that external attributes of a program "should be considered completely reverse engineerable").

to detect copying of the original work, thus undermining the protection offered by copyright.

To date, the courts have been uneven in their treatment of copyright protection for program behavior. In many cases, courts have extended copyright protection to behavioral elements of computer programs, accepting the notion that computer programs ought to receive the same degree of protection from non-literal copying as provided to other literary works.⁷ Other courts, however, have held that program behavior ought to be excluded from the inquiry into non-literal infringement, and have limited their analyses to the non-literal elements of the source code.⁸

The first part of this article develops the reasons for advocating a behavior-based test for determining software copyright infringement, starting with an analysis of the problem in light of traditional copyright doctrine, the Copyright Act of 1976 and congressional intent. Next, the article analyzes how the courts have struggled with the concept of non-literal infringement of computer programs. Most courts appear to be moving toward the Abstraction-Filtration-Comparison (AFC) test which was formulated by the Second Circuit in *Computer Associates International v. Altai*.⁹ While most courts agree on the test, they disagree over its proper application. This article suggests a behavior-based test which modifies the Abstraction-Filtration-Comparison test. The test proposed by this article would eliminate the "abstraction" step of the AFC test, which involves separating the levels of abstraction within the program's code, organization and structure. Instead, the behavior-based test would replace the abstraction step with an "identification" step, which dissects

7. See, e.g., *Whelan Assoc. Inc. v. Jaslow Dental Lab.*, 797 F.2d 1222 (3d Cir. 1986), *cert. denied*, 479 U.S. 1031 (1987) (holding non-literal aspects of program copyrightable); *Broderbund Software v. Unison World, Inc.*, 648 F. Supp. 1127 (N.D. Cal. 1986) (holding sequence of screens, computer screen displays protectable); *Manufacturers Technologies v. Cams, Inc.*, 706 F. Supp. 984, 993 (D. Conn. 1989) (concluding that program's copyright protected the literal and non-literal elements of the program's screen displays, user interface and structure to the extent that each contains copyrightable subject matter); *CMAX/Cleveland v. UCR*, 804 F. Supp. 337 (M.D. Ga. 1992) (holding screen displays and reports were protectable expression); *Apple Computer v. Microsoft Corp.*, 35 F.3d 1435 (9th Cir. 1994) (holding "look and feel" of user interface not protectable expression apart from individual elements of interface); *Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568 (S.D. Fla. 1994) (extending protection to text of commands and the way the program looked, sounded, and interacted with the user); *Autoskill, Inc. v. Nat'l Educ. Support Sys.*, 994 F.2d 1476 (10th Cir. 1993), *cert. denied*, 114 S.Ct. 307 (1994) (finding infringement in reading testing program where infringer had merely changed the names and sequences of the tests and made minor format changes); *Napoli v. Sears, Roebuck and Co.*, 874 F. Supp. 206 (N.D. Ill. 1995) (holding that copyright extends to computer screen displays).

8. See, e.g., *Brown Bag Software v. Symantec*, 960 F.2d 1465 (9th Cir.), *cert. denied*, 113 S. Ct. 198 (1992); *Gates Rubber Co. v. Bando Chemical Indus.*, 9 F.3d 823 (10th Cir. 1993); *Lotus Dev. v. Borland Int'l*, 49 F.3d 807 (1st Cir. 1995), *cert. granted*, 116 S.Ct. 39 (1995).

9. 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part, remanded*, 982 F.2d 693 (2d Cir. 1992).

and identifies the elements of the program's behavior. The behavior-based test would eliminate much of the confusion and difficulty involved with applying the AFC test. Finally, the article applies the proposed test to the facts in *Lotus Development Corp. v. Borland International* to illustrate its advantages. Developing a workable test for non-literal infringement of computer software has become especially relevant in light of the Supreme Court's recent grant of certiorari in the *Lotus* case.¹⁰

II. DEFINING COMPUTER PROGRAM BEHAVIOR

Before beginning any discussion of a test for copyright infringement based on the behavior of computer programs, it will first be necessary to define "program behavior." For purposes of this article, a program's behavior consists of the appearance of the user interface, the way in which the user interacts with the program, the manner in which information is input to and output from the program, and the ensemble of functions provided by the program. In short, it is everything that happens once the program is executed on the target system.

The behavior of a program may be quantified in terms of discrete elements. These elements include the discrete functions performed by the program, specific features of the program's user interface, or particular program responses to a user's actions. A program's behavior can thus be summarized as the set containing all the discrete behavioral elements. Some simple examples of discrete behavioral elements include the manner in which the program responds to specific inputs, such as the invocation of a command by a user, or a signal from the printer indicating that it has run out of paper. A program's response may be expressed as a change in the appearance of the screen, the posting of error messages, or the emission of a beep or other audible signal. Behavior also includes a program's expression in the absence of any input, such as a screen saver program which posts a fluctuating pattern on the computer's screen when the user does nothing. Many programs have very limited or almost no interaction with users, yet still exhibit behavior. An example of this would be a program that controls traffic lights.

10. 116 S.Ct. 39 (1995).

III. FITTING COMPUTER PROGRAMS WITHIN TRADITIONAL COPYRIGHT LAW

A. Behavior Is Expression

In order to be copyrightable, the subject matter must be an "original work of authorship fixed in any tangible medium of expression."¹¹ Copyright law protects an author's expression, rather than merely the idea being expressed. The expression of an idea takes on both substance and form. The substance of the expression lies in the distinction between the author's expression and the ideas which are being expressed. This is the essence of the traditional idea/expression dichotomy of copyright law.¹²

In most cases, the form of the author's expression is readily apparent. For example, the expression of the author of a novel is manifested in the form of printed words on the page. The form of the author's expression, however, can have multiple manifestations, raising the question as to the extent of copyright protection for each distinct manifestation.

The form of the computer programmer's expression can be divided into two distinct manifestations: the literal and the behavioral.¹³ The literal manifestation consists of the text of the human-readable program as written by the programmer (i.e., the source code).¹⁴ The behavioral manifestation consists of the dynamic form of the program as it is being operated on a computer.¹⁵ This bifurcation of expression is neither a new concept nor one unique to computer programs.¹⁶ Consider the various forms of expression of a musical work. The sheet music embodies the literal manifestation of the composer's expression, while the performance of the musical piece makes up the "behavioral" manifestation of that

11. 17 U.S.C. § 102(a) (1988).

12. See *Baker v. Selden*, 101 U.S. 99 (1880); 17 U.S.C. § 102(b) (1988) (codifying the holding of *Baker*, and the idea/expression dichotomy).

13. At least one commentator has expressed the difference as that between interactive and non-interactive elements of the program, defining interactive elements as those which are "directly perceived by humans in the course of using the program." Gross, *supra* note 3, at 112-15.

14. Source code is defined as symbolic coding in its original form before being processed by a computer. The computer automatically translates source code into a code it can understand by a process called "compiling." DONALD SPENCER, WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 539 (5th ed. 1994) [hereinafter WEBSTER'S DICTIONARY OF COMPUTER TERMS].

15. See *supra* part II for a definition of behavior of a computer program.

16. See Pamela Samuelson, *CONTU Revisited: The Case Against Copyright Protection for Computer Programs in Machine-Readable Form*, 1984 DUKE L. J. 663 n.320-22 and accompanying text.

same musical work. Both manifestations are merely alternative forms of the same expression. Thus, each manifestation of the expression should be protected by copyright, because both are a part of the same "original work of authorship." In the case of the musical composition, no one doubts the conclusion that both forms of expression are protected by copyright. The unauthorized public performance of a musical composition infringes the composer's copyright, as does the copying of the sheet music.¹⁷ By analogy, the same reasoning should hold true for computer programs—copying of program behavior infringes the programmer's copyright, as does the copying of the source code.

Computer programs, however, differ from most other literary works in that they derive most of their value from the behavioral form and not from the specific manner in which the programmer implemented the behavior.¹⁸ The behavior of a program may provide a solution to a problem, offer entertainment, or serve as a tool which the user can employ to do valuable work. Consumers would not want to buy a program that does not "behave, i.e., that [does] nothing."¹⁹ Consumers care only about the benefit derived from how the program behaves; the literal manner in which the programmer has implemented the behavior is of little consequence to the consumer.

The literal manifestation of the programmer's expression, on the other hand, only has value to the programmer, who can modify it to maintain and enhance the behavior in subsequent versions of the program.²⁰ Consumers value a program "not because they have any intrinsic interest in what its text says, but because they value what it does and how well it does it."²¹ When a consumer buys a program, he buys only the program's behavior, not the text of the program's source code.²² The consumer cannot directly perceive the programmer's expression from the literal text of the program, because it is invisible to him. Thus, the program behavior represents to the consumer the totality of the programmer's expression.

Given that programs derive so much of their value from their behavioral manifestation, and given that consumers do not perceive the

17. 17 U.S.C. § 106(1) (1988) (providing the author the exclusive right "to reproduce the copyrighted work in copies or phonorecords") and 17 U.S.C. § 106(4) (1988) (providing the author the exclusive right "to perform the copyrighted work publicly").

18. See Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2317 (1994) [hereinafter *Manifesto*].

19. *Id.* at 2315.

20. See Gross, *supra* note 3, at 114-15 ("[T]ypical computer users care very little about a program's non-interactive elements so long as they function properly.").

21. *Manifesto*, *supra* note 18, at 2318.

22. *Id.*

literal manifestation of the program, the emphasis of copyright protection should be aimed at program behavior rather than the written source code.

B. Why Behavior Is Protectable

1. THE 1980 CHANGES TO THE COPYRIGHT STATUTE

When computer programs were explicitly added to the copyright statute in 1980, Congress expressed its intent that such works should be treated as literary works.²³ Though the Copyright Act's definition of a literary works does not expressly list computer programs, the definition clearly encompasses a typical computer program.²⁴ The definition of literary works includes "works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied."²⁵ In addition, a 1976 congressional report explicitly discussed treating computer programs as literary works "to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves."²⁶

Some confusion over the protectability of program behavior may stem from section 101 of the Copyright Act, which defines a computer program as "a set of statements or instructions used directly or indirectly in a computer to bring about a certain result."²⁷ A strict reading of section 101 might suggest that a computer program for copyright purposes is limited to the written source code because the definition under the Act does not expressly refer to a program's behavior or dynamic structure. Yet, the absence of a direct reference to program behavior under section 101 should not be determinative. The language of section 101 can be

23. See CONTU REPORT, *supra* note 2, 18-23. The Congressional Commission on New Technological Uses of Copyrighted Works recommended that the copyright statute be amended to provide protection for computer programs as both literary and audiovisual works. Congress adopted CONTU's recommendations essentially verbatim.

24. A computer program is defined as a formal expression of the sequence of actions required for a data processing task; the programmer's specification of the task(s) to the computer in a formal notation that can be processed by the computer. It consists of a series of statements and instructions that cause a computer to do a specific job. WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 117.

25. 35 U.S.C. § 101 (1988) (definition of "[l]iterary work").

26. H.R. REP. NO. 1476, 94th Cong., 2d Sess. 54 (1976), *reprinted in* 1976 U.S.C.A.N. 5659, 5667 (protecting computer programs as literary works to the extent they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves).

27. 17 U.S.C. § 101 (1988).

interpreted as referring to program behavior indirectly through the phrase "to bring about a certain result."

Furthermore, the use of the defined term "computer program" is conspicuously absent in the section of the Copyright Act defining protectable subject matter, implying that Congress did not intend for computer programs to be treated any differently than other types of literary works. Had Congress intended to limit copyright protection for computer programs as compared to other copyrightable works, it could easily have done so by creating a separate category for computer programs under section 102.²⁸ However, no such attempt was made. The term "computer program" is in fact only used in the copyright statute in section 117,²⁹ which exempts RAM copies created in the owner's operation of a program and copies made for backup purposes from being deemed infringing of the programmer's copyright.³⁰

2. QUASI-LEGISLATIVE HISTORY

Many commentators consider the National Commission of New Technological Uses of Copyrighted Works, Final Report,³¹ (the CONTU Report) to be the quasi-legislative history of the 1980 amendments to the Copyright Act.³² Although not binding, many courts have accepted the report as evidence of congressional intent because the recommendations contained in the CONTU Report were adopted by Congress without alteration.³³ At the time that CONTU prepared its report, "it had been well-established for decades that copyright protection (for literary works)

28. 17 U.S.C. § 102 (1988).

29. 17 U.S.C. § 117 (1988).

30. The statute provides:

Notwithstanding the provisions of § 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:

(1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or

(2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

Id.

31. See CONTU REPORT, *supra* note 2, 18-23.

32. See Arthur J. Levine, *Comment on Bonito Boats Follow-Up: The Likely Rejection of Nonliteral Software Copyright Protection*, 6 COMPUTER L. 29, 31 (1989); *Micro-Sparc, Inc. v. Amtype Corp.*, 592 F. Supp. 33, 35 n.7 (D. Mass. 1984) ("The CONTU Report . . . comprises the entire Legislative history of § 117.").

33. *Whelan Assoc. Inc. v. Jaslow Dental Lab*, 797 F.2d 1222, 1241 (3d Cir. 1986).

extends to non-literal copying as well as to literal copying.³⁴ Thus, had CONTU intended to apply a different standard for determining non-literal infringement for computer programs than for other forms of literary works, the commission could have recommended this in its report. Yet, the CONTU Report recommended that programs be protected as literary works, without any qualification.³⁵ The report expressed the belief that existing copyright principles were adequate for the task of protecting computer programs, suggesting that courts were better equipped than Congress to develop the law through case-by-case decisions, rather than by shortsighted legislative fiat.³⁶

The CONTU commissioners recognized the problem of distinguishing between idea and expression when dealing with a computer program:

Drawing the line between the copyrightable form of a program and the uncopyrightable process which it implements is simple [for pure literal copying]. But the many ways in which programs are . . . used . . . and the new applications which advancing technology will supply may make drawing the line of demarcation more and more difficult. To attempt to establish such a line in this report written in 1978 would be futile. Most infringements, at least in the near future, are likely to involve simply copying . . . Should a line need to be drawn to exclude certain manifestations of programs from copyright, that line should be drawn on a case-by-case basis by the institution designed to make fine distinctions—the federal judiciary.³⁷

The commission's refusal to set a standard has given the courts wide latitude for deciding where the line should be drawn. The fact that commissioners recognized the difficulty in drawing such a line suggests their awareness of the distinction between the literal and behavioral manifestations of computer programs. Had the commissioners wished to exclude the behavior of computer programs from the scope of copyright protection, they would have explicitly done so in their report. Their silence on this point implies the intent to include behavioral aspects of computer programs within the scope of copyright protection. Statements by CONTU Vice-Chairman Melville Nimmer suggest that the above

34. Allen R. Grogan, *Bonito Boats and Whelan: A Simple Contrast Between Patent And Copyright Protection*, 6 *COMPUTER L.* 33, 34 (1989); see also *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930) ("It is essential to any protection of literary property . . . that the right cannot be limited literally to the text, else a plagiarist would escape by immaterial variations.").

35. See CONTU REPORT, *supra* note 2, at 11, 18-23.

36. *Id.* at 21.

37. *Id.* at 23.

interpretation of the CONTU Report is correct.³⁸ Nimmer said he understood CONTU as in no way limiting the application of traditional copyright doctrines to computer programs:

CONTU did not recommend, and did not intend, any change in the continuing applicability to programs of general copyright principles—e.g., as to the copyrightability and infringement—in effect following the enactment of the general revision of the Copyright Act of 1976. The general copyright principles applicable to programs have been, and remain, those which are applicable to novels, plays, directories, dictionaries, textbooks, musical works, maps, motion pictures, sound recordings and other categories of works.³⁹

Thus, CONTU apparently intended that computer programs receive the same level of protection from non-literal infringement as other types of literary works.⁴⁰

3. OTHER LITERARY WORKS WITH BIFURCATED EXPRESSION

Most traditional literary works receive protection from non-literal infringement. Take, for example, "architectural plans, choreography, musical scores, musical editions, and stage direction."⁴¹ All of these works possess bifurcated manifestations of the author's expression, and all receive some degree of copyright protection from non-literal infringement.

Many literary works, besides computer programs, serve primarily utilitarian purposes. Such works include "dictionaries, code books, encyclopedias, advertising, and 'how to' instruction manuals, that, like many computer programs, have a primarily utilitarian, rather than aesthetic, entertainment, or educational purpose."⁴² Copyright nevertheless protects both the literal manifestations and the non-literal

38. See Melville Nimmer, *Declaration Regarding the National Commission on New Technological Uses of Copyrighted Works (CONTU) Final Report* (Nov. 15, 1984) reprinted in Anthony L. Clapes et al., *Silicon Epics And Binary Bards: Determining The Proper Scope Of Copyright Protection For Computer Programs*, 34 UCLA L. REV. 1493, app. (1987) [hereinafter *Nimmer Declaration*].

39. *Id.* at ¶12.

40. However, commissioners Miller and Levine disagree with Nimmer on this point. See Steven R. Englund, Note, *Idea, Process, Or Protected Expression?: Determining The Scope Of Copyright Protection Of The Structure Of Computer Programs*, 88 MICH. L. REV. 866, 888-90 (discussion views of commissioners Miller and Levine).

41. Jane C. Ginsburg, Comment, *Four Reasons and a Paradox: The Manifest Superiority of Copyright Over Sui Generis Protection of Computer Software*, 94 COLUM. L. REV. 2559, 2567 (1994).

42. Arthur R. Miller, *Copyright Protection For Computer Programs, Databases, And Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 986 (1993).

aspects of these works.⁴³ Literary works with utilitarian aspects have been "accorded protection since our first Copyright Act in 1790, which embraced maps and charts."⁴⁴ Thus, a computer program, if treated as a literary work as Congress has mandated, should also be accorded protection of its non-literal aspects, the program's behavior, where such aspects represent the programmer's expression.

4. PURPOSE OF COPYRIGHT

Copyright is a tradeoff which grants an author certain exclusive rights to his work in exchange for the disclosure of the work for the public good.⁴⁵ The exclusive rights granted to the author provide the incentive for the author to create. Thus the valuable aspects of the author's work must be protected from copying; otherwise the author's incentive to create will disappear.

A program which behaves in an identical manner or a very similar manner to another program has the potential of becoming a "market substitute"⁴⁶ for the original program. Such programs may potentially degrade the incentive to the programmer because fewer copies of the original program may be sold in favor of substitute programs. Protection of a program's behavior becomes critical because program behavior plays a significant role in marketing a program to potential purchasers.⁴⁷ The user interface of a program, one element of the program's overall behavior, plays a crucial role in helping consumers to "differentiate a program from among similar software applications in a crowded market."⁴⁸ Taking into consideration that the programmer relies on this aspect of expression to distinguish his program from other competing programs, the necessity of protecting the behavioral manifestation of the programmer's expression from copying becomes readily apparent.

43. *Id.* at 986-87.

44. *Id.* at 986. The author also compares computer programs to architectural works and states that the "recently enacted Architectural Works Copyright Protection Act strikingly echoes the present state of computer copyright law." *Id.* at 988 n.45.

45. See 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §§ 3.01-04.

46. *Manifesto*, *supra* note 18, at 2319; see also Gross, *supra* note 3, at 115 n.28 (even programs that are not identical can compete as substitutes).

47. See Bill Curtis, *Engineering Computer "Look and Feel": User Interface Technology and Human Factors Engineering*, 30 JURI. J. 51, 53 (1989) (discussing the importance of the use interface in marketing software); see also Garard J. Lewis, Jr., Comment, *Lotus Development Corp. v. Paperback Software International: Broad Copyright Protection For User Interfaces Ignores The Software Industry's Trend Toward Standardization*, 52 U. PITT. L. REV. 689, 694-95 n.17 (1991) (citing Curtis).

48. Curtis, *supra* note 47, at 52-54.

Furthermore, limiting copyright protection to program code fails to provide adequate protection for the programmer's creative expression.⁴⁹ Excluding behavior in the determination of non-literal infringement exposes the program's most valuable attributes to copying by any skilled programmer, who could reverse engineer a program by analyzing its behavior and producing an identical or infringing copy without ever viewing the literal source code.⁵⁰ Such reverse engineering often requires only a fraction of the time and labor invested by the programmer of the original work. Ignoring the behavior of a program thus circumvents the very purpose of copyright protection: providing an incentive for the programmer's creative expression for the benefit of the public.

Unlike most other literary works, computer programs are unique in that there is a significant degree of independence between the literal and behavioral manifestations. For most other literary works, the performative manifestation of the work is directly dependent upon the literal manifestation of the work. For example, there is only one way to represent a musical composition in standard musical notation. Likewise, the performance of a play springs directly from the script. For both musical and dramatic works, a change in the literal manifestation of the work has a concomitant effect on the behavioral manifestation. The same cannot be said for computer programs, because there are often numerous ways to write source code to produce a specific behavioral effect.⁵¹ Thus, limiting copyright infringement of computer programs to copying of the source code leaves the programmer with virtually no protection at all. Infringers will be permitted to copy the original programmer's work, so long as they do not copy the original source code.

C. Limitations On Protection Of Behavior

The scope of the protection for computer programs should be identical to the scope for other types of literary works. First, the dichotomy between idea and expression, fundamental to the determination of copyrightability for all types of literary works, should

49. See Margaret L. Pittman, Comment, *What The Judge Sees Is What You Get: The Implications Of Lotus v. Paperback For Software Copyright*, 37 WAYNE L. REV. 1527, 1585 (1991) (noting that limiting copyright protection for computer programs will not effectively protect the programmer's expression).

50. *Manifesto*, *supra* note 18, at 2317-18; see also FAIRLEY, *supra* note 6, at 9 (noting that an estimated 40% of the total development time of a software project is spent on analysis and design, while only 20% is typically spent on implementation (what is termed in this paper "translating the expressive design into literal source code"), debugging and unit testing); see also *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222, 1231 (3d Cir. 1986) ("[T]he coding process is a comparatively small part of programming.").

51. See *Manifesto*, *supra* note 18, at 2315-16. See also Gross, *supra* note 3, at 159 n.229 and accompanying text.

apply to program behavior. Second, the limiting doctrines of merger, *scènes à faire* and originality apply to behavior just as they do to the non-literal aspects of other literary works.

The Supreme Court opinion in the 1879 case of *Baker v. Selden*⁵² developed the modern concept of a dichotomy between idea and expression for determining copyrightability. The Court held that copyright protection for a book describing an accounting system did not extend to the actual accounting system described by the book.⁵³ The alleged infringer, Baker, had used ruled accounting sheets similar to those that had appeared in Selden's book, but had only changed the column headings and arrangement of columns. The Court concluded that the ruled accounting forms were "necessary incidents"⁵⁴ to the use of Selden's accounting system, which was "open and free to the use of the public."⁵⁵ Copyright protection was limited to Selden's particular description of the accounting system. The Court thus distinguished between the unprotectable idea expressed in Selden's book (the accounting system) and the copyrightable expression (Selden's particular description of the accounting system). The principle of *Baker* has since been codified in section 102(b) of the Copyright Act, which states that copyright protection is unavailable for any "idea, procedure, process, system, method of operation, concept, principle, or discovery."⁵⁶

In order to see how *Baker* applies to a computer program, consider the following example. Take a computer program which performs word processing functions. Assume that this word processing program includes a function which allows the printing of addresses on envelopes, a behavioral or non-literal aspect of the program. Under section 102(b), there can be no doubt that copyright protection does not extend to the "idea" of printing addresses on envelopes. Assume further that in order to print the envelopes, the word processing program must undertake the following process: (1) collect the main and return addresses from the user, (2) collect information regarding the size of the envelope from the user, (3) calculate the spacing of the addresses on the envelope, (4) send the spacing information and address information to the printer, and (5) prompt the user to place the envelope into the printer. Any word processing program that offered the function of printing an envelope would have to go through a similar, if not identical, process. Under *Baker*, therefore, this process would be uncopyrightable because it is necessarily incident to the idea of printing an envelope. Furthermore, this sequence

52. 101 U.S. 99 (1879).

53. *Id.* at 104, 107.

54. *Id.* at 103.

55. *Id.* at 101.

56. 17 U.S.C. § 102(b) (1988).

of steps would be expressly excluded from the subject matter copyrightable under section 102(b) because it would be classified as a procedure, process, system or method of operation.

While the idea of printing an envelope and the process used to perform the task are uncopyrightable, the manner in which the program implements the function and process may be considered protectable expression. This would include such things as how the user selects the function, how the program collects necessary information from the user, how the program behaves in case of an error, and so on, subject, of course, to the limiting doctrines of merger, *scènes à faire* and originality. There are multiple ways in which a program could go about performing these tasks. If multiple options for implementation exist, any specific implementation chosen by a programmer cannot be deemed necessarily incident to the idea of the function. Therefore, the particular manner by which the programmer implements the function may be considered the programmer's expression, which falls within the subject matter of copyright. Consider the explanation of this concept in *Baker*:

[T]he teachings of science and the rules and methods of useful art have their end in application and use; and this application and use are what the public derive from the publication of a book which teaches them. But as embodied and taught in a literary composition or book, their essence consists only in their statement. This alone is what is secured by the copyright. The use by another of the same methods of statement, whether words or illustrations, in a book published for teaching the art, would undoubtedly be an infringement of the copyright.⁵⁷

In the example of the envelope-addressing function, the process of printing an envelope is the useful art. The particular manner by which a program implements the function is the "statement" of this useful art, and the "use of another of the same methods of statement" (i.e., an expressive implementation that used the same or substantially similar methods) would be an infringement.⁵⁸

D. Computer Programs As Useful Articles

Objections to the protection of the behavioral aspects of computer programs often focus on the useful article doctrine because computer programs provide utility to their users.⁵⁹ The useful article doctrine of

57. *Baker*, 101 U.S. at 104.

58. See *Nimmer Declaration*, *supra* note 38, at ¶13.

59. See *Manifesto*, *supra* note 18; Leo J. Raskind, *The Uncertain Case For Special Legislation Protecting Computer Software*, 47 U. PITT. L. REV. 1131, 1143-44 (1986) (arguing that programs are uncopyrightable because of their utilitarian nature).

copyright law, articulated by the Supreme Court in *Mazer v. Stein*⁶⁰ and codified in the definition of “[p]ictorial, graphic, and sculptural work” in the current Copyright Act, states,

such works shall include works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned. The design of a useful article . . . shall be considered a pictorial, graphic, or sculptural work only if, and only to the extent that, such design incorporates . . . features that can be identified separately from, and are capable of existing independently of, the utilitarian aspects of the article.⁶¹

There are two responses to those who object to copyright protection for computer programs on the grounds that the programs are “useful articles.” First, any test for copyright infringement of a computer program which applies the limiting doctrines of traditional copyright law will filter out the purely functional aspects of the program. Only particular *implementations* of functions would be protected. Thus, fears that copyright protection for computer programs will give programmers exclusive rights to certain useful arts are unfounded.

Second, the useful article doctrine, as incorporated into the Copyright Act, does not apply to literary works, which include computer programs. The useful article doctrine often has been erroneously generalized to encompass all objects which are the subjects of copyright protection. A strict reading of the copyright statute, however, indicates that the doctrine is intended only to be applicable to pictorial, graphic, or sculptural works.⁶² The definition of these types of works, for copyright purposes, includes only those aspects of the objects which are not utilitarian, but which represent the form, or creative expression, of the creator. The categorization of a computer program as a literary work would thus seem to preclude its definition as a useful article.⁶³

Additionally, while there is no doubt that mere functions are too close to ideas to be copyrightable,⁶⁴ protection is available for sets of

60. 347 U.S. 201 (1954) (holding that statuette of a dancing figure used as a lamp base was copyrightable as a work of art despite being used in a useful object such as a lamp). “Artistic articles are protected in ‘form but not their mechanical or utilitarian aspects.’” *Id.* at 218 (citing 1909 Copyright Act, 17 U.S.C. § 202.8).

61. 17 U.S.C. § 101 (1988).

62. See Jack E. Brown, “Analytical Dissection” Of Computer Software—Complicating The Simple And Confounding The Complex, 25 ARIZ. ST. L. J. 801, 833 (1993) (discussing how the term “useful article” only appears in §§ 101 and 113 of Copyright Act, which pertain to the scope of protection for pictorial, graphic or sculptural works).

63. See *E.F. Johnson Co. v. Uniden Corp. of Am.*, 623 F. Supp. 1485, 1498 (D. Minn. 1985) (rejecting the characterization of plaintiff’s program as “a useful work” and affirming Congress’ decision to treat computer programs as “literary works:” “[T]he limitations placed on the copyrightability of useful articles by section 101 of the Act are simply not applicable here.”).

64. See *supra* part III.C.

functions as compilations. Section 103 of the Copyright Act provides protection for compilations to the extent of the expression contributed by the author,⁶⁵ even if the material that is compiled is not in and of itself copyrightable.⁶⁶ Thus, if a program provides a very unique set of functions, such that the selection of that particular set of functions represents creative expression by the programmer and is not dictated by functional considerations or constraints, then that set of functions is copyrightable. Likewise, protection should be available for compilations of behavior that implement those functions, above and beyond their inherent copyrightability. The court in the case of *Whelan Associates v. Jaslow Dental Laboratory*⁶⁷ supported this notion, noting that sequencing and ordering of materials would also be covered by copyright as compilations, "i.e., that the sequence and order could be parts of the expression, not the idea, of a work."⁶⁸

To date, few courts have used this concept to protect the behavior of programs from copying. The compilation of discrete functions or discrete elements of behavior into a single product that is useful in some way describes the essence of the creative design task of a programmer—the very thing that copyright law is meant to protect.

IV. RELEVANT CASE LAW

The courts have been uneven in their treatment of program behavior. Several courts have recognized copyright protection for some behavioral aspects of computer programs, including such elements as screen displays⁶⁹ and user interfaces.⁷⁰ Other courts have extended non-literal protection to the structure, sequence and organization of a program.⁷¹ Other courts, however, have found program behavior to fall outside the subject matter of copyright.⁷² This lack of consensus among

65. "The copyright in a compilation . . . extends only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work. . . ." 17 U.S.C. § 103(b) (1988).

66. *Miller*, *supra* note 42, at 1003. *See also supra* note 45, at §§ 3.01-04; *Harper House v. Thomas Nelson, Inc.*, 889 F.2d 197, 204-205 (9th Cir. 1989) (uncopyrightable elements of a notebook protectable as a compilation).

67. 797 F.2d 1222 (3d Cir. 1986).

68. *Id.* at 1239.

69. *See Broderbund Software v. Unison World*, 648 F. Supp. 1127, 1132 (N.D. Cal. 1986).

70. *See Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568 1576 (S.D. Fla. 1994).

71. *See Whelan*, 797 F.2d 1222, 1240 (3d Cir. 1986).

72. *See, e.g., Brown Bag Software v. Symantic Corp.*, 960 F.2d 1465 (9th Cir. 1992); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 844 (10th Cir. 1993); *Computer Assoc. Int'l. v. Altai*, 775 F. Supp. 544, 560 (E.D.N.Y. 1991), *aff'd*, 982 D.2d 693 (2nd Cir. 1992).

the courts has led to confusion over the protectability of program behavior.

The courts that have upheld copyright protection for behavioral elements of programs have taken notice of the fact that behavior represents the programmer's expression. These courts have realized that behavioral elements are "as valuable, if not more valuable, than the program code and structure itself and, therefore, warrant protection."⁷³ For example, in *Lotus Development Corp. v. Paperback Software International*,⁷⁴ the court expressed concern that if the scope of protection for computer programs is too narrow, "copyright law never would, as a practical matter, provide computer programs with protection as substantial as Congress has mandated—protection designed to extend to original elements of expression *however embodied*."⁷⁵

In *Whelan Associates v. Jaslow Dental Laboratory*,⁷⁶ the Third Circuit took an important first step toward recognition of the behavioral aspects of programs. The court noted that other literary works could be infringed through non-literal copying, citing the example that "[o]ne can violate the copyright of a play or book by copying its plot or plot devices."⁷⁷ The court then drew the conclusion by analogy that the copyright of a program could be infringed "even absent copying of the literal elements of the program."⁷⁸ The court made its analysis within the framework of the traditional idea/expression dichotomy of *Baker* and section 102(b) of the Copyright Act, deciding that the idea expressed by the programmer was the function of the program, with the actual program being the programmer's expression of that idea.⁷⁹ The court reasoned that since there were a variety of ways in which the program could have been implemented, "the [dynamic] structure is not a necessary incident to that idea,"⁸⁰ and was therefore copyrightable expression. The court also relied on public policy to reach this conclusion, noting that "we must remember that the purpose of the copyright law is to create the most efficient and productive balance between protection (incentive) and dissemination of information, to promote learning, culture and development."⁸¹

73. John Houston, Comment, *A Unified Test For The Copyright Protection Of The User Interface To Computer Programs*, 32 DUQ. L. REV. 133, 142 (1993).

74. 740 F. Supp. 37 (D. Mass. 1990).

75. *Id.* at 56 (emphasis added).

76. 797 F.2d 1222 (3d Cir. 1986).

77. *Id.* at 1234.

78. *Id.*

79. *Id.* at 1238-40.

80. *Id.* at 1240.

81. *Id.* at 1235.

While the *Whelan* court has been widely criticized for providing over-broad protection for programs, the court nonetheless correctly concluded that the non-literal aspects of a program are protectable under copyright.⁸² *Whelan* provides the basis for an argument that non-literal aspects of a program—in other words, the program behavior—are copyrightable.

Though the courts continue to disagree over the proper scope of copyright protection for computer programs, most courts appear to agree upon the Abstraction-Filtration-Comparison (AFC) test, formulated in *Computer Associates International v. Altai, Inc.*,⁸³ as the proper test for non-literal infringement of computer programs. The Second Circuit's AFC test has been adopted in some form by the Fifth Circuit,⁸⁴ the Ninth Circuit,⁸⁵ the Tenth Circuit,⁸⁶ the Federal Circuit,⁸⁷ and by district courts in the Eleventh Circuit.⁸⁸

The district court in *Altai* expressly took notice of the bifurcated nature of the programmer's expression in computer programs:

Each view—textual and behavioral—has its own structure, sequence, and organization. In the standard jargon of programmers, there is static structure, which refers to the program-as-text view, and dynamic structure, which refers to the program-as-behavior view. The static structure and dynamic structure of a program can be quite different; indeed from dealing with the behavior of a program, i.e., operating it, one can tell virtually nothing about its text. Thus . . . "it makes no technical sense to talk simply about the 'structure' of a program, because the term is ambiguous and the distinction [between dynamic structure and static structure] matters."⁸⁹

82. See, e.g., Englund, *supra* note 40; Michael A. Jacobs, *Copyright and Compatibility*, 30 JURI. J. 91 (1989); Andrew O. Martyniuk, Comment, *Abstraction-Filtration-Comparison Analysis and the Narrowing Scope of Copyright Protection for Computer Programs*, 63 U. CIN. L. REV. 1333 (1995); Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045 (1989); Pamela Samuelson, *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, 6 HIGH TECH. L. J. 209 (1991); Peter G. Spivak, Comment, *Does Form Follow Function? The Idea/Expression Dichotomy in Copyright Protection of Computer Programs*, 35 UCLA L. REV. 723 (1988); Nicholas P. Terry, *GUI Wars: The Windows Litigation and the Continuing Decline of "Look And Feel"*, 47 ARK. L. REV. 93, 142, n.222-24 (1994).

83. 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part, remanded*, 982 F.2d 693 (2d Cir. 1992).

84. *Engineering Dynamics v. Structural Software, Inc.*, 26 F.3d 1335, 1342-43 (5th Cir. 1994); *Kepner-Tregoe, Inc. v. Leadership Software, Inc.*, 12 F.3d 527, 536-37 (5th Cir. 1994).

85. *Apple Computer v. Microsoft Corp.*, 35 F.3d 1435, 1442-43 (9th Cir. 1994).

86. *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 834 (10th Cir. 1993); *Autoskill v. Nat. Educ. Support Sys.*, 994 F.2d 1476, 1487-98 (10th Cir. 1993).

87. *Atari Games Corp. v. Nintendo of Am.*, 975 F.2d 832, 839 (Fed. Cir. 1992).

88. *Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568, 1577-78 (M.D. Fla. 1994); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337, 352-54 (M.D. Ga. 1992).

89. *Altai*, 775 F. Supp. at 559-60.

The *Altai* court criticized *Whelan* as being "inadequate and inaccurate" for ignoring the distinction between the static and dynamic structure of a program, and for assuming that a program is the expression of a single idea, instead of the expression of multiple ideas.⁹⁰

The *Altai* court, however, wrongly expressed doubts as to the copyrightability of a program's "dynamic structure"—in other words, the behavioral manifestation of the program. The *Altai* court's misgivings over the protectability of program behavior stemmed from its misinterpretation of section 102(b) of the Copyright Act.⁹¹ The district court stated that "since the behavior aspect of a computer program falls within the statutory terms 'process,' 'system,' and 'method of operation,' it may be excluded by statute from copyright protection."⁹² Yet, the court stopped short of holding as a matter of law that program behavior was a system, process or method of operation, thereby leaving the door open for copyright protection of program behavior. The *Altai* court held that the plaintiff's rights were fully protected by examining the literal program code, thus permitting the court to avoid determining whether program behavior should be excluded from the subject matter of copyright.⁹³ Thus the district court left the issue of the protectability of program behavior for another court, or for Congress, to decide.

In affirming the district court in *Altai*, the Second Circuit panel devised the three-step AFC test⁹⁴ for determining infringement of computer programs based on the abstraction test devised by Judge Learned Hand in the case of *Nichols v. Universal Pictures*,⁹⁵ which involved a non-literal infringement claim by an author of a play against the producer of another play. The AFC test applies concepts of traditional copyright law such as the idea/expression dichotomy and the limiting doctrines of merger, *scènes à faire* and originality to computer programs. As such, it is seen by many as a narrowing of the protection for non-literal aspects of computer programs after *Whelan*.⁹⁶ Nonetheless, *Altai* affirms that traditional copyright law principles are applicable to the non-literal aspects of computer programs. *Altai's* AFC test also provides an appropriate framework upon which a test for infringement can be built.

90. *Id.* at 559.

91. "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work." 17 U.S.C. § 102(b) (1988).

92. *Altai*, 775 F. Supp. 544 at 560.

93. *Id.*

94. See *infra* part VI.

95. 45 F. 2d 119, 121 (2d Cir. 1930).

96. See *supra* note 68 and accompanying text.

The behavior-based test proposed in this article is a modification of the AFC test.⁹⁷

Since *Altai*, several other courts have upheld protection for non-literal behavioral aspects of computer programs.⁹⁸ In the case of *Autoskill v. National Educational Support Systems*,⁹⁹ the Tenth Circuit applied the *Altai* test and determined that a program implementing a reading system was infringed by another program which simply changed the names and sequences of tests in the operation of the infringing program. In *Mitek Holdings v. Arce Engineering Co.*,¹⁰⁰ the district court, in applying the *Altai* test, determined that some non-literal, behavioral elements of the allegedly infringed program were protectable.¹⁰¹ The court concluded, however, that there was not enough similarity to make a finding of infringement.¹⁰² Though the court found no infringement, the significance of *Mitek* lies in the court's recognition that some behavioral elements were found to be protectable.

In *Apple Computer v. Microsoft*,¹⁰³ the Ninth Circuit identified similarities between discrete behavioral elements in both the copyrighted and allegedly infringing programs.¹⁰⁴ The Ninth Circuit, however, held there was no infringement because most of the similarities were permitted by a license agreement between the plaintiff and the defendant, or were obvious expressions of basic ideas, and thus precluded from copyright protection by the merger doctrine.¹⁰⁵ As such, the court felt that infringement could only be found if the works as a whole were virtually identical.¹⁰⁶ This case provides yet another example of an instance where a court has embraced the notion that behavioral elements of a program are protectable, though infringement was not found.

Other courts, however, have followed the dicta in *Altai*, concluding that protection from non-literal infringement does not extend to program behavior. In *Gates Rubber Co. v. Bando American, Inc.*,¹⁰⁷ the district court explicitly held that the behavior of a computer program was protectable:

The court will respectfully disagree with the *Altai* decision and hold that a program's behavior can be protected by copyright law [T]he

97. See *infra* part VI.

98. See *supra* note 7.

99. 994 F.2d 1476 (10th Cir. 1993).

100. 864 F. Supp. 1568 (S.D. Fla. 1994).

101. *Id.* at 1577-78.

102. *Id.* at 1580.

103. 35 F.3d 1435 (9th Cir. 1994).

104. *Id.* at 1438.

105. *Id.* at 1446.

106. *Id.* at 1447.

107. 798 F. Supp. 1499 (D. Colo. 1992), *vacated and remanded in part, aff'd in part*, 9 F.3d 823 (10th Cir. 1993).

commonality of [the] error denotes "behavior" as to how one part of the program works with another. This is *part of the creative expression* of the program itself.¹⁰⁸

The Tenth Circuit reversed, however, holding that the district court had failed to properly eliminate the behavioral elements of the program from the determination of infringement.¹⁰⁹

The First Circuit decision in the case of *Lotus Development Corp. v. Borland International*¹¹⁰ further confused the issue of protectability of behavior. The First Circuit, in reversing the district court's finding that the menu command structure of the plaintiff's program was protectable, held that menu command structure was a "method of operation" and therefore uncopyrightable under section 102(b).¹¹¹ The court stated that the *Altai* test was applicable to non-literal copying, but that the appropriation of the menu command structure represented literal copying, and thus the *Altai* test did not apply.¹¹² What the court failed to take into account, however, was that the literally copied portion of the program was in reality a non-literal behavioral aspect of the program.

Given the uneven treatment by the courts, the protectability of behavioral aspects of programs remains uncertain. Much of the difficulty lies in agreeing upon the common terminology to describe literal and non-literal aspects of a program. The disagreement, however, appears ripe for a decision by the Supreme Court.¹¹³

V. THE PROPOSED BEHAVIOR-BASED TEST

The test advocated by this article would look solely at the behavioral manifestation of the programmer's expression and would ignore the literal manifestation when determining whether infringement has occurred.¹¹⁴ Once the behavioral elements have been isolated, the proposed behavior-based test would apply the idea/expression dichotomy and traditional copyright limiting doctrines such as merger, *scènes a faire* and originality to determine which behavioral elements deserve copyright protection and which elements ought to be excluded. The behavioral elements of the original work would then be compared

108. *Id.* at 1518-19 (emphasis added).

109. 9 F.3d 823 at 835.

110. 49 F.3d 807 (1st Cir. 1995).

111. *Id.* at 815.

112. *Id.* at 814.

113. The Supreme Court has granted a writ of certiorari in the *Lotus* case. *Lotus Dev. Corp. v. Borland Int'l*, 116 S.Ct. 39 (1995).

114. If a program is literally copied (i.e. the source code of the program is duplicated) then the behavior of the copy would be identical to the behavior of the original, and would thus infringe under this test.

with the behavioral elements of the infringing program to determine whether there is substantial similarity between them. A test of this nature makes more sense in light of the nature and realities of computer programs and the public policy surrounding traditional copyright law.

A good starting point for defining such a test is the AFC test articulated by the Second Circuit in *Computer Associates International, v. Altai, Inc.*¹¹⁵ This test has been adopted, in one form or another, by several courts in cases involving infringement of non-literal aspects of computer programs.¹¹⁶ The *Altai* test consists of a three-step procedure which is used to determine if an allegedly infringing program is substantially similar to the allegedly infringed program.

In ascertaining substantial similarity under this approach, a court would first break down the allegedly infringed program into its constituent structural parts. Then, by examining each of these parts for such things as incorporated ideas, expression that is necessarily incidental to those ideas, and elements that are taken from the public domain, a court would then be able to sift out all non-protectable material. Left with a kernel, or possible kernels, of creative expression after following this process of elimination, the court's last step would be to compare this material with the structure of an allegedly infringing program. The result of this comparison will determine whether the protectable elements of the programs at issue are substantially similar so as to warrant a finding of infringement.¹¹⁷

1. ABSTRACTION

The abstraction step, described above as "break[ing] down the allegedly infringed program into its constituent structural parts," requires the court to reconstruct the programmer's implementation of the program in reverse order.

115. 982 F.2d 693, 706-711 (2d Cir. 1992).

116. See, e.g., *Lotus Dev. Corp. v. Borland Int'l*, 49 F.3d 807, 816 (1st Cir. 1995), cert. granted, 116 S.Ct. 39 (1995) ("*Altai* test may provide a useful framework for assessing the alleged nonliteral copying of computer code."); *Lotus Dev. Corp. v. Borland, Int'l.*, 799 F. Supp. 203 (D. Mass. 1992) (concluding that the test developed by the district court was "compatible substantively, though different in methodology" than the *Altai* test); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 828 (10th Cir. 1993) ("In substantial part, we adopt the 'Abstraction-Filtration-Comparison' test."); *Productivity Software Int'l. v. Healthcare Tech.*, 1995 WL 437526 (S.D.N.Y. 1995) (using *Altai* test to determine substantial similarity); *Triad Sys. Corp. v. Southeastern Express Co.*, 31 U.S.P.Q.2d (BNA) 1239, 1248 (N.D. Cal. 1994) (using first two steps of the *Altai* test for distinguishing between protectable expression and unprotectable ideas, processes, etc., where substantial similarity was not disputed); *Atari Games Corp. v. Nintendo of Am., Inc.*, 30 U.S.P.Q.2d 1401 (BNA) (N.D. Cal. 1993) ("In our view, in light of the essentially utilitarian nature of computer programs, the Second Circuit's approach is an appropriate one.").

117. *Altai*, 982 F.2d at 706.

Initially, in a manner that resembles reverse engineering on a theoretical plane, a court should dissect the allegedly copied program's structure and isolate each level of abstraction contained within it. This process begins with the code and ends with an articulation of the program's ultimate function. Along the way, it is necessary essentially to retrace and map each of the designer's steps—in the opposite order in which they were taken during the program's creation.¹¹⁸

This step of the test requires that the court acquire knowledge equivalent to that of a computer program developer, a requirement which is beyond the capability of most courts. As a result, expert analysis and testimony is usually required to assist the court in performing the abstraction step of the test.

The proposed behavior-based test would eliminate the abstraction step of the *Altai* test. The first step of the test would instead involve identifying the discrete elements which represent the program's behavior. Call this the "identification" step. The court should identify the behavioral elements of a computer program simply by operating the program on a computer. This will permit observation of how the program behaves. For example: "the program performs functions X, Y and Z" or "when the user does this, the program responds by doing that." The level of complexity of the observations is a function of the complexity of the program. For a more complicated program, instead of observing "when the user does this, the program does that," it may be necessary to observe that "when the user does this, and conditions A, B and C are met, then the program does that."

As an example, it may be helpful to consider the small icon resembling a trash-can which appears on the lower right hand corner of the Apple Macintosh user interface. When a user uses the mouse to drag a file icon into the trash-can icon, the file icon is prepared for deletion from the computer's disk. This description of the trash-can icon and its function identifies a certain behavioral element of the program which generates the user interface of the Apple Macintosh. Thus, the first step of the behavior-based test has been completed.

2. FILTRATION

The second step of the *Altai* test, the filtration step, requires the court to apply traditional limiting doctrines of copyright law to the abstractions formulated in the first step of the test. It is described as "examining each of these parts for such things as incorporated ideas, expression that is necessarily incidental to those ideas, and elements that are taken from the public domain." In essence, the court is to apply the

118. *Id.* at 707.

doctrines of merger, *scénès a faire* and originality to the various levels of abstraction.

This process entails examining the structural components at each level of abstraction to determine whether their particular inclusion at that level was an "idea" or was dictated by considerations of efficiency, so as to be necessarily incident to that idea [merger doctrine]; required by factors external to the program itself [*scénès a faire* doctrine]; or taken from the public domain [originality requirement] and hence is nonprotectable expression.¹¹⁹

The purpose of this test is to "filter out" subject matter that is unprotectable. After the application of this step of the test, the fact finder is left with the protectable expression of the allegedly infringed program.

The *Altai* court first applied the merger doctrine to the abstracted structure of the program. The principle underlying the merger doctrine was well-stated by the First Circuit in the *Concrete Machinery Co. v. Classic Lawn Ornaments, Inc.*¹²⁰ The court stated, "[w]hen there is essentially only one way to express an idea, the idea and its expression are inseparable and copyright is no bar to copying that expression."¹²¹ The *Altai* court also applied this doctrine to computer programs, stating, "[i]n the computer context, this means that when specific instructions, even though previously copyrighted, are the only and essential means of accomplishing a given task, their later use by another will not amount to infringement."¹²²

The proposed behavior-based test would apply the merger doctrine as stated in *Concrete Machinery* to the behavioral elements of the program which were observed in the identification step of the test. Continuing with the above example of the Apple Macintosh trash-can icon, one can imagine an almost infinite number of ways in which the function which deletes a file from the computer's disk could be implemented. The trash-can icon is therefore not rendered unprotectable by the merger doctrine.

The *Altai* court then applied the "*scénès a faire*" doctrine. This doctrine states that when external factors constrict the possible ways to express an idea, such expression is not protectable by copyright. Professor Nimmer, in his treatise on copyright law, has identified five instances of external factors which may circumscribe the manner in which a program is designed.¹²³ The *Altai* court adopted these factors.¹²⁴ They are: (1) the mechanical specifications of the computer on which a particular program

119. *Id.*

120. 843 F.2d 600 (1st Cir. 1988).

121. *Id.* at 606.

122. *Altai*, 982 F.2d at 708.

123. 3 NIMMER & NIMMER, *supra* note 45, at 13-65.

124. *Altai*, 982 F.2d at 709.

is intended to run; (2) compatibility requirements of other programs with which a program is designed to operate in conjunction; (3) computer manufacturer's design standards; (4) demands of the industry being serviced; and (5) widely accepted practices within the computer industry.¹²⁵

The proposed behavior-based test adopts these factors as well, but applies them to the observations of the identification step of the test, instead of to the level of structural abstractions identified in the abstractions step of the *Altai* test. In the example of the trash-can icon, it is unlikely that any of the five factors listed above would require that a user interface allow users to delete files from the computer's disk in this fashion.

Finally, the *Altai* court applied the originality standard to the levels of abstraction. This limitation is based on the statutory requirement that copyright protect only "original works of authorship."¹²⁶ In the context of a computer program, this excludes from protection material which is taken from the public domain. The *Altai* court stated, "Such material is free for the taking and cannot be appropriated by a single author even though it is included in a copyrighted work."¹²⁷

The proposed behavior-based test also adopts this standard, as applied to the discrete behavioral elements of the program observed in the identification step of the test. Returning yet again to the trash-can icon example, assuming that Apple is the originator of this particular feature, its copyrightability would be unaffected by the filtration step of the test.

3. COMPARISON

The final step of the *Altai* test is the comparison step. The court described this step of the test as, "whether the defendant copied any aspect of this protected expression, as well as an assessment of the copied portion's relative importance with respect to the plaintiff's overall program."¹²⁸

The proposed behavior-based test also includes this step of the *Altai* test. The discrete behavioral elements of the alleged infringing program are to be compared with the discrete behavioral elements of the allegedly infringed program which are copyrightable, i.e., those that remain after the filtration step. The comparison should be performed both in terms of quantity and quality of copying. In other words, if the infringing program copied substantial portions of the original program, then a finding of

125. *Id.*

126. 17 U.S.C. § 102(a) (1988).

127. *Altai*, 982 F.2d at 710.

128. *Id.* at 710.

infringement is warranted. Likewise, if only a small portion has been copied but the portion copied is qualitatively substantial, that is, the particular behavior copied makes the original program particularly valuable and desirable to consumers, then a finding of infringement may also be warranted.

VI. AN APPLICATION OF THE PROPOSED BEHAVIOR-BASED TEST

To illustrate how the proposed behavior-based "Identification-Filtration-Comparison" test operates, it may be useful to look at its application to a real case. The case of *Lotus Development Corp. v. Borland International*¹²⁹ provides a good opportunity to examine behavioral elements of a computer program.

The dispute in the case arose when Borland copied portions of the Lotus 1-2-3 spreadsheet program in its own spreadsheet product. Specifically, Borland included in its product a mode which emulated the menu command structure of 1-2-3. The menu command structure is the part of the user interface of the program which allows users to input commands to the program.¹³⁰ Additionally, the 1-2-3 menu command structure also facilitated the running of 1-2-3 user-written macros.¹³¹ The Borland spreadsheet product permitted its users to operate the program in a mode which copied the 1-2-3 menu command structure. This served two purposes. First, it allowed users who were familiar with the 1-2-3 menu command structure to easily switch to the Borland product. Secondly, it allowed users who had written macros for 1-2-3 to run those macros from within the Borland product. The Borland product also featured a "Key Reader" facility which allowed the running of the 1-2-3

129. 788 F. Supp. 78 (D. Mass. 1992), 799 F. Supp. 203 (D. Mass. 1992), 831 F. Supp. 202 (D. Mass. 1992), 831 F. Supp. 223 (D. Mass. 1992), *rev'd.*, 49 F.3d 807 (1st Cir. 1995), *cert. granted*, 116 S.Ct. 39 (1995).

130. A menu is a list of command options available to the user of a program. See WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 365. The menu command structure of 1-2-3 consists of a series of commands, spaced horizontally across the top of the screen, from which the user can select, using the computer's mouse or keyboard. These commands are the top of a tree of commands available to the user. When one of these commands is selected, a sub-menu of commands, or another branch in the tree of commands, appears. Each item in the sub-menu that the user could select is either another branch in the tree of commands, leading to another sub-menu, or a leaf of the tree, representing a command which tells the program to perform a specific function.

131. A macro is a single command, made up by a user, which can replace a series of the 1-2-3 commands. A user can define a series of 1-2-3 commands, and assign a name to the series. This "macro" can then be invoked by using the assigned name, instead of having to enter each 1-2-3 command in the series individually. See WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 351.

macros even when the 1-2-3 menu command structure was not being used.

The district court in the case found that the Borland product infringed the 1-2-3 product. To make this determination, the court used a test which it claimed was compatible with the *Altai* Abstraction-Filtration-Comparison test.¹³² The First Circuit Court of Appeals subsequently overturned this decision, stating that the 1-2-3 menu command structure was a "method of operation" and was thereby uncopyrightable under the copyright statute.¹³³ The Supreme Court has since granted certiorari on the case.¹³⁴

In applying the "Identification-Filtration-Comparison" test outlined above, the first step is to observe the behavior of the program and identify its behavioral elements. There is no doubt that the operation of the menu command hierarchy is a behavioral element, or several behavioral elements of the 1-2-3 program. When a user selects any item in any sub-menu, the 1-2-3 program responds with a specific response, either the posting of a new sub-menu, or the invocation of a program function. In a complete analysis of the case, the court would be required to identify all of the behavioral elements of the program, including the layouts of the screens, the manner in which the functions of the program are carried out, how error messages are posted, etc. For purposes of this example, however, we will stop at the observation that the menu command structure represents a set of discrete behavioral elements of the 1-2-3 program which, if not filtered out by the next step of the test, are copyrightable as the expression of the programmer.

The filtration step of the test determines if any of the behavioral elements observed in the identification step of the test should be rendered unprotectable because of the application of one of the limiting doctrines of copyright law. It does not appear that there is any merger of idea and expression with regard to the menu command structure. The manner in which the Lotus designers implemented the menu command structure of 1-2-3 is certainly not the only way that it could be done. The existence of the alternate method used by the Borland product proves this. Likewise, we will assume that the design of the 1-2-3 menu command structure was original to the Lotus designers.

The application of the *scènes à faire* doctrine, however, raises issues as to the copyrightability of the menu command structure. One of the factors identified by Nimmer and adopted by the *Altai* court was "compatibility requirements of other programs with which a program is

132. *Lotus*, 799 F. Supp. at 223-23, 831 F. Supp. at 245.

133. *Lotus*, 49 F.3d at 815.

134. *Lotus*, 116 S.Ct. 39 (1995).

designed to operate in conjunction." In this case, the Borland program wishes to allow its users to run the macros they have created using the 1-2-3 program. There is no way to allow the running of the 1-2-3 macros without the menu command structure being recreated in one form or another. The copying of the menu command structure represents a design constraint of making the Borland product compatible with the 1-2-3 program. Thus, the discrete behavioral elements making up the 1-2-3 menu command structure must be filtered out from the set of protectable behavioral elements of the 1-2-3 program.

The application of the comparison step of the test is moot at this point because all of the behavioral elements which have been copied by the alleged infringing Borland program have been filtered out of the set of copyrightable behavioral elements of the 1-2-3 program. Thus, there can be no infringement.

VII. CONCLUSION

Some commentators have argued that protection for computer programs would be better provided under patent law¹³⁵ or a sui generis intellectual property regime.¹³⁶ This article, however, suggests that copyright law is flexible enough to accommodate new creative works like computer programs by applying traditional copyright doctrines and weighing modern public policy objectives. Furthermore, a copyright regime that denies a programmer protection from copying of the behavioral aspects of his programs is tantamount to providing him no protection whatsoever. This article has presented several arguments why such protection is necessary and suggested a method by which courts may properly carry out the congressional mandate to extend copyright protection to computer programs.

135. Mark A. Lemley, *Convergence in the Law of Software Copyright*, 10 HIGH TECH. L.J. 1 at 26 (1995) ("Altering copyright law rather than employing patent protection has arguably overprotected computer software . . .").

136. See generally *Manifesto*, *supra* note 18.

BOOK REVIEW

DNA IN THE COURTROOM: A TRIAL WATCHER'S GUIDE

**by HOWARD C. COLEMAN & ERIC D. SWENSON
GENELEX PRESS, SEATTLE, WA; 131 PAGES; \$12.95**

REVIEWED BY JASMINE SAMRAD †

Scientific technologies have expanded exponentially in our century, leaving virtually no aspect of our lives unaffected. Nowhere is this more obvious than in our courtrooms, which have turned into science battlegrounds where ever more complex technologies are introduced as evidence. These new technologies challenge us not only to grasp their scientific complexity but also to evaluate their reliability as evidence. One of the seminal challenges in the field of scientific evidence has been the struggle to assimilate the revolutionary new DNA technologies, especially DNA fingerprinting, into the legal system. Nevertheless, until the O.J. Simpson trial drew the nation's attention to the controversy, few people outside the relevant legal and scientific fields were aware of its scope and significance.

The much-publicized battle between Simpson's defense team and prosecutors regarding DNA evidence was, however, only a relatively minor skirmish in an ongoing "DNA War" over the introduction of this revolutionary forensic technology into our courtrooms. Since soon after the technique's discovery in 1985, proponents of DNA fingerprinting have battled critics who questioned the reliability of the technique, the interpretation of results and their admissibility in criminal trials. Many of the criticisms initially raised, such as proper testing procedures and statistical analysis methods, have since been addressed or refuted, and the technology has gathered widening support in the scientific community. Nevertheless, some critics have persisted in their attacks, perpetuating the confusion and controversy. The debates have highlighted not only the complexities of DNA

© 1995 Jasmine Samrad.

† J.S.D. Candidate, 1997, LL.M., 1995, Boalt Hall School of Law, University of California, Berkeley. J.D., School of Law, 1993, B.S., 1989, University of California, Davis.

fingerprinting evidence, but also the difficulty of incorporating scientific evidence into our present judicial structure.

*DNA in the Courtroom: A Trial Watcher's Guide*¹ by Howard Coleman and Eric Swenson is a handy primer on the DNA controversy, covering the technology of DNA fingerprinting and the legal treatment of DNA evidence. Coleman is president of GeneLex Corporation, a nationally recognized laboratory that performs DNA testing for both forensic analysis and determination of parentage.² Swenson is a professional writer and teacher of technical writing. The collaboration of these two authors results in a thorough, technically accurate yet eminently readable work that will be of interest to a broad audience. The book's original purpose, to provide a technical guide for reporters covering the Simpson trial, evidences itself in the lucidity and accessibility of its presentation. The work is a welcome resource in this highly charged area of both scientific and legal complexity. Although the book is especially appropriate for those with no scientific or legal background who need a clear and concise introduction to DNA fingerprinting, the book is comprehensive enough to offer insights even to those with strong knowledge in the field.

SYNOPSIS

DNA in the Courtroom: A Trial Watcher's Guide contains six short chapters that provide a historical account of the major battles in the DNA war, explain the science and technology of forensic DNA fingerprinting and discuss treatment of DNA under the law of scientific evidence. The book includes a chapter specifically on the Simpson trial, which is not as superfluous as one might think even at this late date, and a useful appendix listing the status of DNA fingerprinting in forty-seven states with relevant case law.

Chapter One chronicles the major battles of the DNA controversy and is one of the most intriguing and entertaining sections of the book. Coleman, himself a DNA expert with extensive experience testifying and teaching about forensic and parentage DNA testing, provides a blow-by-blow, front-line view of the DNA controversy. His account mirrors other reports³ in portraying the

1. HOWARD C. COLEMAN & ERIC D. SWENSON, *DNA IN THE COURTROOM: A TRIAL WATCHER'S GUIDE* (1994).

2. Determination of paternity, maternity, or other kinship is referred to as "parentage testing."

3. See, e.g., William C. Thompson, *Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War,"* 84 J. CRIM. L. & CRIMINOLOGY 22, 100-03 (1993).

controversy as unusually acrimonious, with both proponents and opponents of DNA evidence often resorting to attacking the qualifications and the character of opposing experts, rather than attacking the evidence itself. Coleman attributes the contentiousness of the DNA fingerprinting controversy to several factors: the commercial motives of the labs that developed the technologies, the "contentious and fragmented nature of our legal system," and inaccurate media coverage.⁴

The introduction of this revolutionary technology into the courtroom by private companies, an element unique in the history of forensic science, played a key role in creating and perpetuating the controversy. These companies' pursuit of commercial goals created an environment unfavorable to the introduction of a technology with such vast potential for changing the criminal justice system.⁵ The major private laboratories were engaged in a race to the courtroom, attempting to license their procedures and sell their products to as many forensic laboratories as possible.⁶ The companies strove to gain a competitive advantage by keeping their products and technologies secret.⁷ The normal procedures for validating new scientific methods, such as publication, peer review and standardization, were bypassed in the commercial laboratories' rush to get a return on their substantial investment and start-up costs.⁸ Moreover, companies used different tools and procedures, which precluded easy comparison of results between companies.⁹

This commercially competitive climate delayed the development of adequate quality control and validity standards.¹⁰ Meanwhile the private companies, aided by "an adulatory press," avidly promoted the new technology to the bench, the bar and law enforcement.¹¹ Thus DNA fingerprinting initially enjoyed a nearly meteoric rise to stardom in the forensic science landscape. Courts and commentators almost universally accepted and hailed DNA fingerprinting as a reliable and accurate identification tool that promised to revolutionize the criminal justice system.¹² A stunned

4. COLEMAN & SWENSON, *supra* note 1, at 1.

5. *Id.* at 4.

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *See id.* at 5.

11. *Id.*

12. *See id.* *See also* THOMPSON, *supra* note 3, at 22; ANDRE A. MOENSSSENS ET AL., SCIENTIFIC EVIDENCE IN CIVIL AND CRIMINAL CASES 938 (4th ed. 1995).

defense bar, caught unawares, made few objections and viewed the new technology as virtually impossible to defend against.¹³ Soon, however, defense attorneys rallied and delivered their first major victory against the admissibility of DNA fingerprints in the landmark case *People v. Castro*.¹⁴ Thus began the so-called "DNA Wars."

Coleman and Swenson deliver a succinct summary of *Castro* and the major arguments propounded against admitting the DNA fingerprinting evidence. Jose Castro was charged with the murder of a pregnant women and her daughter after DNA from blood found on Castro's watch was found to match the woman's DNA. The trial court in *Castro* excluded the DNA evidence inculpatating Castro after experts from both the prosecution and defense testified that the DNA fingerprints were obtained under flawed conditions and were therefore unreliable.¹⁵ No appellate opinion on whether flawed DNA testing conditions preclude admissibility ever materialized since, soon after the DNA evidence was excluded, Castro confessed to the crime and pled guilty.¹⁶ Nevertheless, *Castro's* impact remained substantial; DNA evidence and the laboratories that performed them could no longer be viewed as infallible.

Castro was the spark igniting the powder keg of controversy that became known as the "DNA Wars." *DNA in the Courtroom* describes the DNA battles as they were fought in the courts, in academic circles and in the media, where the press had a field day bashing the technology it had previously called a miracle.

Coleman and Swenson claim the media fueled the DNA controversy through sensational, misleading or downright inaccurate reporting.¹⁷ One example comes from the *New York Times's* coverage of

13. COLEMAN & SWENSON, *supra* note 1, at 5.

14. 144 Misc. 2d 956 (N.Y. 1989).

15. See COLEMAN & SWENSON, *supra* note 1, at 6. The court found that the theories underlying DNA fingerprinting were reliable enough to render DNA evidence generally admissible, but that inaccuracies in performance of the tests rendered these particular match results too unreliable to be admitted. These inaccuracies included the laboratory's apparent inculpatory bias when drawing conclusions from ambiguous data, failure to use adequate controls to verify that interpretations were correct, ignoring the failure of some controls that were used, THOMPSON, *supra* note 3, at 43, and failure to adequately correct for bacterial contamination, Thomas M. Fleming, Annotation, *Admissibility of DNA Identification Evidence*, 84 A.L.R. 4th 313, 331-32 n.56 (1991). Courts today continue to split over the significance of proper performance of testing procedures. Some hold that performance of the technique goes to the weight, rather than the admissibility, of the test results, while other courts require proper performance of tests before the DNA evidence can be admitted. MOENSENS, *supra* note 12, at 942-43.

16. COLEMAN & SWENSON, *supra* note 1, at 6.

17. See *id.* at 13-14.

the important National Research Council report, *DNA Technology in Forensic Science*.¹⁸ The report explicitly recommended the *continued use* of DNA fingerprints in court, emphasizing only the need to apply adequate quality control protocols and recommending a conservative (pro-defendant) method of statistical analysis.¹⁹ However, the *Times* completely misrepresented the report's findings as advocating a *ban* on DNA evidence until the scientific basis was stronger.²⁰

In addition to irresponsible media coverage and the commercial interests of the private companies, other elements also played a role in perpetuating the confusion and controversy regarding DNA fingerprints. The authors mention as exacerbating factors the strategies and politics of both the prosecution and defense bar,²¹ and the expert witnesses who often have a vested interest in perpetuating the controversy so their services will still be needed.²² The authors plainly believe that the DNA controversy was largely overblown and unnecessarily exacerbated by all of these factors. However, one of the book's weaknesses is its failure to acknowledge the benefits resulting from the controversy. The authors do seem to concede that focusing national attention on the importance of standardization and quality control did provide some gains. For example, the authors note that the FBI's creation of a national DNA laboratory caused the "standardization of a chaotic industry."²³ However, they fail to analyze the possible connection between the rising tide of criticism against DNA fingerprints, defense victories like *Castro* and the development of such national DNA laboratories.

Coleman and Swenson expressly state in their preface that they are strong proponents of admitting DNA evidence. Perhaps because of this perspective, the general tone of the book seems to blame the perpetuation of the controversy largely on the defense bar and its experts. The authors seem to suggest that the defense bar sometimes went beyond proper zealous advocacy to the point of intentionally muddying the waters and confusing the issues. If this is their view,

18. *Id.*

19. *Id.* See generally COMMITTEE ON DNA TECHNOLOGY IN FORENSIC SCIENCE, NATIONAL RESEARCH COUNCIL, *DNA TECHNOLOGY IN FORENSIC SCIENCE* (1992).

20. COLEMAN & SWENSON, *supra* note 1, at 13.

21. See *id.* at 16-18. The authors also argue that the DNA controversy has been exacerbated by a "politicization" of the judicial process, where prosecutors "adopt a bunker mentality when under attack while doing their job of protecting us from criminals, [while defense attorneys] feel under siege because they usually have even fewer resources... than does the prosecution" and must fulfill their role of safeguarding individual liberties. *Id.* at 16-17.

22. *Id.* at 18.

23. *Id.* at 7.

they are by no means alone. Nonetheless, the authors make an obvious attempt to present a balanced view, identifying errors by all involved parties, including the prosecution, the media, the judiciary and the scientific community.

The remaining chapters of the book describe the science behind DNA fingerprinting and the use of DNA evidence in the courtroom. In chapters Two and Three, the authors provide an explanation of the theory and practice of DNA fingerprinting; these two chapters are exemplary in their thoroughness and accessibility. Readers need no scientific literacy whatsoever to grasp the explanations offered here. The authors supplement their descriptions with helpful lay analogies and extremely useful charts and diagrams.

Chapter Two describes DNA evidence as a tool in the field of forensic serology, explaining the possible sources of DNA, such as blood, semen, or hair roots,²⁴ and comparing DNA typing with the other major types of serological evidence such as traditional blood typing and human leukocyte antigen (HLA) analysis. DNA evidence presents several advantages over traditional types of blood analysis. For example, DNA is very durable, being less susceptible to environmental degradation and physical and biological contamination than other components of blood evidence. DNA testing can also indicate when a crime scene sample is a mixture from several sources, and can often separate out different individuals' DNA from the mix. Of course, DNA can identify or exclude a suspect with much higher confidence than any other available test because it provides more precise information.²⁵

Chapter Three details the scientific underpinnings and technical procedures for obtaining a DNA fingerprint. DNA fingerprinting allows highly accurate identification of individuals by isolating and identifying certain sequences of DNA whose length and number vary greatly from person to person, and comparing the pattern of these DNA sequences found in crime samples with a suspect's pattern to determine if the DNA patterns match.²⁶ The authors explain the

24. *Id.* at 20-22.

25. *See id.* at 25-27.

26. In the procedure called RFLP (Restriction Fragment Length Polymorphism) analysis, these DNA fragments are separated by size using an electrical current which pulls smaller fragments farther through a porous gel than larger fragments. The resulting series of DNA bands are radioactively tagged and then made visible by exposure to a sheet of film. The resulting "picture" is a column of bands positioned according to size and superficially resembling the UPC bar code found on commercial goods. By comparing the band pattern of a crime scene sample with the patterns from the victim and any suspects, technicians will determine if any of the DNA in the sample matches that of a suspect. Once a match, or inclusion, is declared, the

basic genetic principles which allow DNA fingerprinting to work and thoroughly cover the various steps performed in obtaining a DNA fingerprint and declaring a match. The discussion includes an extensive description of what promises to be the foremost DNA analysis technique in the near future, PCR-based typing. PCR typing is based on a procedure, called polymerase chain reaction amplification, that increases the amount of available DNA by duplicating it over and over. PCR analysis presents several advantages over traditional (RFLP) analysis, being a faster and relatively simpler operation that can be performed on even minute amounts of DNA.²⁷

Once one of these testing methods yields a match between the suspect's DNA pattern and the pattern found in the crime scene sample, the suspect is said to be "included" in the class of possible perpetrators of the crime. An inclusion does not, however, automatically mean that the suspect committed the crime, since someone else with the same DNA pattern may have been the actual perpetrator. The likelihood that someone else with the same DNA pattern may have been the source of the crime scene sample is determined by statistical analysis of the occurrence of that particular DNA pattern in the general population. Thus if a DNA pattern appears with high frequency in the population, a match between a suspect and a crime scene sample will be less significant than if the pattern appears infrequently. Moreover, DNA fingerprints usually test for several different DNA sequences. Each DNA sequence has its own frequency of occurrence in the general population. The overall frequency for a DNA fingerprint that tests multiple sequences is calculated by multiplying the individual frequencies of each DNA sequence.²⁸ This frequency calculation method is called the product rule.

Statistical analysis methods such as the product rule are at the center of a maelstrom of controversy in the DNA wars. Critics argue that the product rule underestimates the frequency of the suspect's DNA pattern in the general population, thus overestimating the

statistical likelihood that the defendant is not the source (i.e., that the match occurred randomly) is evaluated using population databases which estimate the frequency of the tested DNA fragments in the population.

27. See MOENSSENS, *supra* note 12, at 910-12.

28. Thus, if a DNA fingerprint tests for sequence A and sequence B, and the individual frequency of sequence A in the general population is 1 in 100, or .01, and the frequency of sequence B is 1 in 1000, or .001, the frequency of a DNA fingerprint showing both A and B will be $.001 \times .01 = .00001$ or 1 in 100,000. Clearly, as more sequences are tested for, the frequency for the overall DNA pattern can quickly reach one in millions or even billions.

likelihood that the suspect is the source of the crime scene sample DNA. These critics argue that analysis of the frequency of DNA patterns in the general population, or even in specific ethnic populations, ignores the possibility of smaller subpopulations in which the frequency of the suspect's DNA pattern may occur with greater frequency than in the larger population.²⁹ Proponents of DNA evidence counter that no evidence shows that the existence of subpopulations significantly alters the frequency calculations.³⁰ Furthermore, proponents have proposed alternatives to the product rule that are conservative (pro-defendant) methods of statistical analysis that more than account for any unknown bias such as the subpopulation problem.³¹ Critics have responded by attacking these alternative methods as inaccurate calculations that violate population genetics principles.³² Some renowned scientists, attempting to quiet the storm of controversy, point out that although the alternative methods may not be the *best* statistical evaluation method, they are so conservative that no one could argue that their inaccuracy harms the defendant.³³

One weakness of the book is its relatively cursory treatment of this statistical analysis controversy. A satisfactory overview of this issue and the complex field of population genetics is an admittedly difficult task given the scope of the book. Nevertheless the importance of this element of DNA evidence and its starring role in the current DNA debates calls for more comprehensive coverage than the authors provide.

The authors next include a short chapter on DNA parentage testing. Although they have received far less press and have not figured significantly in the debates on DNA fingerprinting reliability, parentage testing cases are the most common application of the technology.³⁴ DNA parentage testing applications include child support enforcement, criminal paternity, identifying human remains and medical genetics.³⁵ Parentage DNA testing, like forensic DNA analysis, has considerable advantages over conventional blood analysis, but also shares with forensic DNA testing the same difficulties that can affect reliability, such as proper performance of

29. See MOENSSENS, *supra* note 12, at 924-25.

30. See *id.* at 925-26.

31. See *id.* at 926-27.

32. See *id.* at 927-28.

33. See, e.g., Eric S. Lander & Bruce Budowle, *DNA Fingerprinting Dispute Laid to Rest*, 371 NATURE 735 (1994).

34. COLEMAN & SWENSON, *supra* note 1, at 62.

35. *Id.* at 64.

testing procedures, chain of custody, degraded samples, laboratory quality control and statistical population analysis. Interestingly, opponents of forensic DNA testing have not been as vocal in attacking the reliability of DNA testing for parentage purposes.³⁶ This is true even though parentage tests often provide evidence in criminal cases, for example by identifying human remains or testing fetuses for proof of criminal activity such as rape or child molestation.³⁷ The lack of opposition is even more surprising considering that the proficiency of testing laboratories is less closely scrutinized and more susceptible to variations in quality in parentage testing than in the forensic setting.³⁸ This selectivity in criticism may, as the authors point out, provide insight into the true significance of many of the objections to forensic DNA testing.

The discussion then moves from the complexities of DNA technology in the laboratory to the complexities of DNA technology in the courtroom. In chapter Five the authors reach the crux of the DNA controversy: the difficulties of incorporating complex scientific evidence into our legal system. In their description of the relevant legal rules governing DNA admissibility, the authors conscientiously explain all legal provisions in lay terms. They succinctly describe the nature of evidence, including rules on opinion testimony and expert opinions, as well as basic principles of discovery.³⁹ The authors describe how discovery has sometimes been a source of contention, but focus on admissibility as the central legal issue in DNA fingerprinting.⁴⁰

The DNA controversy centers on the admissibility of DNA fingerprints at trial. Scientific evidence, such as DNA fingerprints, must meet a certain reliability threshold before it can be admitted.⁴¹ The rationale for this special evidentiary standard is that scientific evidence, by its very nature, is not susceptible to the adversarial system's traditional measures for ensuring reliability, such as cross-examination and opposing evidence. Factfinders, whether judge or jury, do not have the requisite technical knowledge to evaluate the reliability of the scientific evidence. In fact, this is the very reason such evidence is needed in the first place, to provide the factfinder with technical knowledge and information it does not itself possess.

36. The same conspicuous silence is evident when forensic DNA testing is used to exculpate the defendant.

37. See COLEMAN & SWENSON, *supra* note 1, at 66-67.

38. *Id.* at 70-71.

39. *Id.* at 75-77.

40. *Id.* at 77.

41. See *id.*

In addition, such evidence can often have an aura of infallibility that can so overwhelm factfinders, especially lay juries, that they may afford the evidence disproportionate weight.⁴²

Courts have applied various standards to measure the reliability of scientific evidence. The authors provide a concise account of these standards and their historical development. Courts today determine admissibility using either the *Frye* rule, which requires that scientific evidence must be "generally accepted" by the scientific community before being admitted,⁴³ or the Federal Rules of Evidence (FRE) which require that scientific evidence be relevant⁴⁴ and helpful.⁴⁵

Until 1993 it was unclear whether the FRE, which nowhere mention general acceptance, had superseded the *Frye* rule. Some federal circuits held that the FRE abolished *Frye*, while others read the FRE as incorporating the *Frye* rule into their reliability requirement.⁴⁶ The United States Supreme Court resolved the split in the recent landmark case *Daubert v. Merrell Dow Pharmaceuticals*, holding that *Frye* did not survive the enactment of the FRE that

42. DNA fingerprints clearly carry this aura since the match frequencies are so astronomical that they seem to prove indisputably the defendant's guilt.

43. COLEMAN & SWENSON, *supra* note 1, at 77. The *Frye* rule originated in a 1923 federal court of appeals decision that excluded the results of a primitive lie-detector test as too unreliable. *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). In a much-quoted statement, the court declared:

Just when a scientific principle or discovery crosses the line between experimental and demonstrable stages is difficult to define. Somewhere in the twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.

Frye, 293 F. at 1014.

44. FED. R. EVID. 402.

45. FED. R. EVID. 702 ("If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise."). Helpfulness incorporates reliability since unreliable evidence will not be helpful. See *Daubert v. Merrell Dow Pharmaceuticals*, *infra* note 47. The FRE are directly applicable only to federal courts, but many states have evidence codes patterned after, and identical in relevant part, to the FRE.

46. States with evidence codes patterned after the FRE were similarly struggling to reconcile the FRE and *Frye*. Like the federal courts, these states split on whether their evidence codes superseded *Frye*.

scientific evidence is to be evaluated using the FRE's relevance and helpfulness standard.⁴⁷

In addition to covering these various evidentiary rules, the authors note two additional legal standards affecting DNA admissibility, the emergence in some states of legislated admissibility and the role of expert witnesses. Several states have enacted statutes mandating the admissibility of DNA evidence without antecedent expert testimony on the technique's reliability.⁴⁸ This legislated admissibility applies only to the underlying theories and technology of DNA fingerprinting, not issues such as statistical evaluation methods or proper performance of testing protocols that currently are the primary points of contention.⁴⁹ Nor do the statutes apply to subsequently developed DNA analysis methods.⁵⁰ Nevertheless, legislated admissibility promises to be a growing trend in the field.⁵¹

Our legal system's reliance on partisan experts to bring scientific evidence to the courtroom also has a profound effect on DNA admissibility. Coleman and Swenson make note of the proliferation of "professional experts" who are not always well-qualified or impartial enough to be relied on to provide the court with such complex and often outcome-determinative material as DNA evidence. Some suggestions for curtailing this phenomenon include implementing rigorous academic, professional and ethical qualification requirements for expert witnesses and increased use of court-appointed experts to promote impartiality.⁵²

The authors next present a section, highly useful to practitioners, describing defense strategies and the main lines of attack on forensic DNA testing. The authors survey the primary points of contention, including experts' conflicts of interest, unreliable chain of custody,

47. 113 S. Ct. 2786, 2794 (1993). Like the FRE, *Daubert* does not automatically control state evidentiary law, but since many state codes are identical to the FRE in relevant part, such states may choose to follow the U.S. Supreme Court's interpretation of the FRE and *Frye*. Some of these states had already abandoned *Frye* for the federal approach pre-*Daubert*. See, e.g., *Prater v. State*, 820 S.W.2d 429 (Ark. 1991); *Santiago v. State*, 510 A.2d 488 (Del. 1986); *Rivera v. State*, 840 P.2d 933 (Wyo. 1992). Others have since adopted the *Daubert* reasoning and abolished *Frye*. See, e.g., *City of Fargo v. McLaughlin*, 512 N.W.2d 700 (N.D. 1994); *State v. Alberico*, 861 P.2d 192 (N.M. 1993). The remainder have yet to reject *Frye* in favor of *Daubert*.

48. COLEMAN & SWENSON, *supra* note 1, at 80. In their appendix, the authors list these states, which include Alabama, Connecticut, Indiana, Louisiana, Maryland, Minnesota, Nevada, Tennessee, Virginia, and West Virginia. See *id.* at 113-20.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.* at 81-82.

technical inaccuracies (such as improper procedures or contamination of samples) and unreliable statistical analysis methods.⁵³ Unfortunately, as in the technical chapters, the authors provide insufficient coverage of the now-dominant statistical analysis controversy.

The authors briefly survey the trial and appeals processes. They review several appellate-level decisions regarding DNA admissibility. The authors also survey several California appellate decisions, concluding that California courts unanimously accept the theory and methods of RFLP testing, but differ in their rulings on admissibility of statistical analysis results.⁵⁴

Finally, the authors discuss the role of DNA fingerprints in providing relief from erroneous convictions. The authors state that about a dozen men have had convictions reversed and been released from prison when DNA evidence excluded them as the perpetrators of the crime for which they had been convicted.⁵⁵ According to the authors, an additional thousand men annually are arrested as crime suspects and then released without being charged when DNA evidence exonerates them.⁵⁶ The authors note that also some of the most vociferous objectors to admitting *inculpatory* DNA evidence ardently advocate use of DNA evidence to *exculpate* the accused.⁵⁷ This dichotomy is certainly interesting. The point would be even more telling if the authors critically evaluated the justifications put forth by those who propose this dual standard, an evaluation the authors do not undertake.

With regard to inculpatory evidence, the authors note that, despite the contention surrounding DNA fingerprinting, the injustices predicted by opponents of the evidence have failed to materialize. For example, the record shows no re-test of DNA evidence resulting in inconsistent conclusions from the original analysis.⁵⁸

The final chapter of the book covers the early stages of the Simpson trial, as the prosecution and defense teams were gearing up for the battle over DNA evidence. While one might be tempted to dismiss this chapter as irrelevant now that the trial is over, the discussion is actually an absorbing case study of the contours of a DNA battle. The authors present an analysis of defense and prosecution strategies, as well as detailed commentary regarding the experts

53. *Id.* at 82-86.

54. *See id.* at 88-89.

55. *Id.* at 89.

56. *See id.* at 112.

57. *Id.* at 90.

58. *Id.* at 90.

lined up on either side. The description of the experts, their backgrounds, qualifications and personalities, enlivens the discussion and illuminates how these elements impact the experts' testimony and contribute to the contentious nature of the DNA controversy. This perspective is particularly relevant since the experts employed in the Simpson case are some of the main players in the DNA controversy and will continue to figure prominently as the debates continue.

CONCLUSION

The authors, in their afterword, conclude that "the prospects for ending the DNA War quickly are dim."⁵⁹ Although they believe that developments in the technology will eventually compel complete acceptance of DNA evidence, they oppose deferring the use of such a powerful tool until absolutely no scientific disagreements exist. They note that "[t]he DNA revolution has brought into sharp focus how hard it is for the judicial system to evaluate and incorporate new scientific technologies,"⁶⁰ and posit that the DNA controversy "speak[s] more to the nature of our legal system and the politics and economics of the scientific community than to the soundness of the technology."⁶¹

Knowledge and information are the key to a better understanding of these revolutionary technologies. Jurists can no longer afford the scientific illiteracy that so characterizes the legal field. *DNA in the Courtroom* counteracts this phenomenon of illiteracy by providing a concise, yet comprehensive, introduction to the complex scientific and legal issues of DNA fingerprinting. The work is worthwhile, entertaining and accessible reading for jurists, journalists and the general public alike.

59. *Id.* at 111.

60. *Id.* at 112.

61. *Id.*

INDEXES

The following indexes include references to all articles and comments published in Volumes 1-10. These indexes allow the reader to locate articles and comments by author's name, issue of publication, subject matter or title. Similar indexes, linked to abstracts for each article and comment, appear on the High Technology Law Journal's site on the World Wide Web at <http://server.berkeley.edu/HTLJ/>.

TABLE OF CONTENTS

AUTHOR INDEX.....	447
ISSUE INDEX.....	460
SUBJECT INDEX.....	466
TITLE INDEX	475

AUTHOR INDEX

A

Ausubel, Warren

- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Issue 4:1 (Spring 1989)

B

Barkan, David

- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, Issue 7:2 (Fall 1992)

Bayer, Barry

- *Computerized Citation Checking Revisited*, Issue 3:2 (Fall 1988)

Beard, Joseph

- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Issue 8:1 (Spring 1993)

Bell, Suzanne

- *Software Product Liability: Understanding and Minimizing the Risks*, Issue 5:1 (Spring 1990)

Berring, Robert

- *Full-Text Databases and Legal Research: Backing Into the Future*, Issue 1:1 (Spring 1986)

Brooks, Timothy

- *Regulating International Trade in Launch Services*, Issue 6:1 (Spring 1991)

Burgunder, Lee

- *An Emerging Theory of Computer Software Genericism*, Issue 2:2 (Fall 1987)

C**Cabot, Howard Ross**

- *Watercloud Muddies the Water for Patent Coverage Disputes*, Issue 8:2 (Fall 1993)

Carleton, Dennis M.

- *A Behavior-Based Model for Determining Software Copyright Infringement*, Issue 10:2 (Fall 1995)

Crisman, Thomas

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Cross, George

- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Issue 1:2 (Fall 1986)

Cunningham, Brian

- *Emerging Product Liability Issues in Biotechnology*, Issue 3:2 (Fall 1988)

D**Danilenko, Gennady**

- *Outer Space and the Multilateral Treaty-Making Process*, Issue 4:2 (Fall 1989)

Darr, Frank

- *Regulation of Alternative Operator Services*, Issue 6:1 (Spring 1991)

Debessonnet, Cary

- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Issue 1:2 (Fall 1986)

Denemark, Howard

- *The Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth,"* Issue 8:2 (Fall 1993)

Dorney, Maureen

- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Issue 5:2 (Fall 1990)

Douros, Timothy J.

- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Issue 10:2 (Fall 1995)

E**Eisenschmidt, Lori E.**

- *The Commercial Law of Internet Security*, Issue 10:2 (Fall 1995)

F**Feldman, Miles**

- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Issue 9:1 (Spring 1994)

Fought, Bonnie

- *Legal Aspects of the Commercialization of Space Transportation Systems*, Issue 3:1 (Spring 1988)

Fox, Eleanor

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Issue 6:1 (Spring 1991)

G**Gill, Christopher**

- *Medical Expert Systems: Grappling with Issues of Liability*, Issue 1:2 (Fall 1986)

Gruner, Richard

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Issue 1:2 (Fall 1986)

H**Hasan, Salim A.**

- *A Call for Reconsideration of the Strict Utility Standard in Chemical Patent Practice*, Issue 9:2 (Fall 1994)

Heckman, Carey

- *An Emerging Theory of Computer Software Genericism*, Issue 2:2 (Fall 1987)

Herman, Karen Goldman

- *Issues in the Regulation of Bioengineered Food*, Issue 7:1 (Spring 1992)

Hertz, Ellen

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Issue 5:2 (Fall 1990)

Hogle, Doreen

- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Issue 5:1 (Spring 1990)

Hurewitz, Barry J.

- *Non-Proliferation and Free Access to Outer Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Issue 9:2 (Fall 1994)

I J**Johnson, Dana**

- *The Impact of International Law and Treaty Obligations on United States Military Activities in Space*, Issue 3:1 (Spring 1988)

Johnston, Sean

- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Issue 4:2 (Fall 1989)

Johnston, Pamela

- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Issue 2:2 (Fall 1987)

Jones, Richard

- *Is There a Property Interest in Scientific Research Data?*, Issue 1:2 (Fall 1986)

Jorde, Thomas

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Issue 4:1 (Spring 1989)

K**Kasch, Steven**

- *The Semiconductor Chip Protection Act: Past, Present, and Future*, Issue 7:1 (Spring 1992)

Koffsky, Mark

- *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Issue 9:1 (Spring 1994)

Krauthaus, Patricia

- *Secured Financing and Information Property Rights*, Issue 2:2 (Fall 1987)

Kuo, John

- *Sales/Use Taxation of Software: An Issue of Tangibility*, Issue 2:1 (Spring 1987)

Kushan, Jeffrey

- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Issue 6:1 (Spring 1991)

L**Lacroix, Gerard**

- *Protecting the "Look and Feel" of Computer Software*, Issue 1:2 (Fall 1986)

Lagod, Martin

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Issue 5:2 (Fall 1990)

Larson, Alexander

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Issue 6:2 (Fall 1991)

Lee, Mavis

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Issue 6:2 (Fall 1991)

Lee, Michele

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Issue 6:2 (Fall 1991)

Lemley, Mark A.

- *Convergence in the Law of Software Copyright?*, Issue 10:1 (Spring 1995)

Levy, Lawrence

- *Software Product Liability: Understanding and Minimizing the Risks*, Issue 5:1 (Spring 1990)

Loewenheim, Ulrich

- *Legal Protection for Computer Programs in West Germany*, Issue 4:2 (Fall 1989)

Lunney, Glynn

- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Issue 5:1 (Spring 1990)

M**Maatz, Claire Turcotte**

- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Issue 7:1 (Spring 1992)

Manheim, William

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, Issue 2:1 (Spring 1987)

Martin, Patricia

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Issue 5:2 (Fall 1990)

May, Randolph

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Issue 8:1 (Spring 1993)

McGarity, Thomas

- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Issue 9:1 (Spring 1994)

McGraw, Molly

- *Sound Sampling Protection and Infringement in Today's Music Industry*, Issue 4:1 (Spring 1989)

McManis, Charles

- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Issue 8:1 (Spring 1993)

McNally, Janine

- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Issue 5:1 (Spring 1990)

Meeker, Heather J.

- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Issue 9:2 (Fall 1994)

Merges, Robert

- *Uncertainty and the Standard of Patentability*, Issue 7:1 (Spring 1992)
- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Issue 3:1 (Spring 1988)

Methvin, Gaynell

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Michel, Suzanne

- *The Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, Issue 7:2 (Fall 1992)

N**Naumann, Adrienne**

- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Issue 1:1 (Spring 1986)

Nicholson, Bradley J.

- *The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM*, Issue 10:1 (Spring 1995)

Nimmer, Raymond

- *Secured Financing and Information Property Rights*, Issue 2:2 (Fall 1987)

O P**Pace, Kimberly**

- *The Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, Issue 9:1 (Spring 1994)

Paepke, C. Owen

- *An Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, Issue 2:1 (Spring 1987)

Paredes, Troy

- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?* Issue 9:2 (Fall 1994)

Pinheiro, John

- *Protecting the "Look and Feel" of Computer Software*, Issue 1:2 (Fall 1986)

Poulter, Susan

- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Issue 7:2 (Fall 1992)

Q R**Reisman, Joseph**

- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Issue 10:2 (Fall 1995)

Reynolds, Glenn

- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Issue 3:1 (Spring 1988)

Rich, Allen

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Robinson, George

- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, Issue 3:1 (Spring 1988)

Rosenkranz, E. Joshua

- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, Issue 2:1 (Spring 1987)

Rosler, Debra B.

- *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, Issue 10:1 (Spring 1995)

Rowland, Bertram

- *Legal Implications of Letter Licenses for Biotechnology*, Issue 1:1 (Spring 1986)

Rustad, Michael

- *The Commercial Law of Internet Security*, Issue 10:2 (Fall 1995)

S**Samuelson, Pamela**

- *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Issue 6:2 (Fall 1991)

Schroepfer, Terrence

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Issue 6:2 (Fall 1991)

Seecof, Benjamin

- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Issue 5:2 (Fall 1990)

Selbak, John

- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, Issue 9:2 (Fall 1994)

Silverman, Alexander

- *Intellectual Property Law and the Venture Capitalist Process*, Issue 5:1 (Spring 1990)

Steele, Lisa

- *The View From on High: Satellite Remote Sensing Technology and the Fourth Amendment*, Issue 6:2 (Fall 1991)

Stockdale, Donald

- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost*, Issue 7:2 (Fall 1992)

Stork, Anita

- *The Use of Arbitration in Copyright Disputes: IBM v. Fujitsu*, Issue 3:2 (Fall 1988)

Stovsky, Michael

- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Issue 6:2 (Fall 1991)

Sullivan, Lawrence A.

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Issue 5:2 (Fall 1990)

Sullivan, Barry

- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Issue 3:2 (Fall 1988)

T**Teece, David**

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Issue 4:1 (Spring 1989)

Thomas, John R.

- *The Question Concerning Patent Law and Pioneer Inventions*, Issue 10:1 (Spring 1995)

Traynor, Michael

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Issue 6:1 (Spring 1991)
- *Emerging Product Liability Issues in Biotechnology*, Issue 3:2 (Fall 1988)

U V W X Y Z**Weitz, David**

- *The Biological Deposit Requirement: A Means of Assuring Adequate Disclosure*, Issue 8:2 (Fall 1993)

Welch, Mark

- *Computerized Citation Checking Revisited*, Issue 3:2 (Fall 1988)

Whitt, Richard

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Issue 8:1 (Spring 1993)

Winters, Steven

- *The New Privacy Interest: Electronic Mail in the Workplace*, Issue 8:1 (Spring 1993)

Wrenn, Gregory

- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Issue 4:2 (Fall 1989)

Wright, Christopher

- *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, Issue 1:1 (Spring 1986)

Yin, Tung

- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Issue 8:2 (Fall 1993)

Zschau, Ed

- *Export Controls and America's Competitive Challenge*, Issue 1:1 (Spring 1986)

ISSUE INDEX

Issue 10:2

- *The Commercial Law of Internet Security*, Michael Rustad and Lori E. Eisenschmidt
- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Timothy J. Douros
- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Joseph M. Reisman
- *A Behavior-Based Model for Determining Software Copyright Infringement*, Dennis M. Carleton

Issue 10:1

- *Convergence in the Law of Software Copyright?*, Mark A. Lemley
- *The Question Concerning Patent Law and Pioneer Inventions*, John R. Thomas
- *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, Debra B. Rosler
- *The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM*, Bradley J. Nicholson

Issue 9:2

- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Heather J. Meeker
- *Non-Proliferation and Free Access to Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Barry J. Hurewitz
- *A Call for Reconsideration of the Strict Utility Standard in Chemical Patent Practice*, Salim A. Hasan
- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?*, Troy Paredes
- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, John Selbak

Issue 9:1

- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Thomas McGarity

- *The Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, Kimberly Pace
- *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Mark Koffsky
- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Miles Feldman

Issue 8:2

- *The Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth,"* Howard Denmark
- *Watercloud Muddies the Water for Patent Coverage Disputes*, Howard Ross Cabot
- *The Biological Deposit Requirement: A Means of Assuring Adequate Disclosure*, David Weitz
- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Tung Yin

Issue 8:1

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Randolph May and Richard Whitt
- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Charles McManis
- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Joseph Beard
- *The New Privacy Interest: Electronic Mail in the Workplace*, Steven Winters

Issue 7:2

- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Susan Poulter
- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost?*, Donald Stockdale
- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, David Barkan

- *The Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, Suzanne Michel

Issue 7:1

- *Uncertainty and the Standard of Patentability*, Robert Merges
- *The Semiconductor Chip Protection Act: Past, Present, and Future*, Steven Kasch
- *Issues in the Regulation of Bioengineered Food*, Karen Goldman Herman
- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Claire Turcotte Maatz

Issue 6:2

- *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Pamela Samuelson
- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Alexander Larson and Terrence Schroepfer
- *The View From on High: Satellite Remote Sensing Technology and the Fourth Amendment*, Lisa Steele
- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Mavis Lee and Michele Lee
- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Michael Stovsky

Issue 6:1

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Eleanor Fox and Michael Traynor
- *Regulation of Alternative Operator Services*, Frank Darr
- *Regulating International Trade in Launch Services*, Timothy Brooks
- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Jeffrey Kushan

Issue 5:2

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Lawrence A. Sullivan and Ellen Hertz

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Patricia Martin
- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Allen Rich, Gaynell Methvin and Thomas Crisman
- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Maureen Dorney
- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Benjamin Seecof

Issue 5:1

- *Software Product Liability: Understanding and Minimizing the Risks*, Lawrence Levy and Suzanne Bell
- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Glynn Lunney
- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Doreen Hogle
- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Janine McNally
- *Intellectual Property Law and the Venture Capitalist Process*, Alexander Silverman

Issue 4:2

- *Legal Protection for Computer Programs in West Germany*, Ulrich Loewenheim
- *Outer Space and the Multilateral Treaty-Making Process*, Gennady Danilenko
- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Sean Johnston
- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Gregory Wrenn

Issue 4:1

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Thomas Jorde and David Teece
- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Warren Ausubel

- *Sound Sampling Protection and Infringement in Today's Music Industry*, Molly McGraw

Issue 3:2

- *Emerging Product Liability Issues in Biotechnology*, Michael Traynor and Brian Cunningham
- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Barry Sullivan
- *The Use of Arbitration in Copyright Disputes: IBM v. Fujitsu*, Anita Stork
- *Computerized Citation Checking Revisited*, Mark Welch and Barry Bayer

Issue 3:1

- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Robert Merges and Glenn Reynolds
- *The Impact of International Law and Treaty Obligations on United States Military Activities in Space*, Dana Johnson
- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, George Robinson
- *Legal Aspects of the Commercialization of Space Transportation Systems*, Bonnie Fought

Issue 2:2

- *Secured Financing and Information Property Rights*, Raymond Nimmer and Patricia Krauthaus
- *An Emerging Theory of Computer Software Genericism*, Lee Burgunder and Carey Heckman
- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Pamela Johnston

Issue 2:1

- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, E. Joshua Rosenkranz
- *An Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, C. Owen Paepke

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, William Manheim
- *Sales/Use Taxation of Software: An Issue of Tangibility*, John Kuo

Issue 1:2

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Richard Gruner
- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Cary Debessonet and George Cross
- *Protecting the "Look and Feel" of Computer Software*, John Pinheiro and Gérard Lacroix
- *Is There a Property Interest in Scientific Research Data?*, Richard Jones
- *Medical Expert Systems: Grappling with Issues of Liability*, Christopher Gill

Issue 1:1

- *Export Controls and America's Competitive Challenge*, Ed Zschau
- *Full-Text Databases and Legal Research: Backing Into the Future*, Robert Berring
- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Adrienne Naumann
- *Legal Implications of Letter Licenses for Biotechnology*, Bertram Rowland
- *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, Christopher Wright

SUBJECT INDEX

The references to each article in the list below include the authors' last names and the issue number. For example, Martin/Lagod 5:2 indicates an article written by Martin and Lagod that appeared in HTLJ issue 5:2.

A

- **abortion:** Martin/Lagod 5:2, Meeker 9:2
- **abstraction-filtration comparison test:** Lemley 10:1
- **active review:** Poulter 7:2
- **alternative operator services:** Darr 6:1
- **antitrust law:** Jorde/Teece 4:1, Lee/Lee 6:2, Lunney 5:1, Paredes 9:2, Stockdale 7:2, Sullivan/Hertz 5:2, Wright 1:1
- **arbitration:** Rich 5:2, Stork 3:2
- **artificial intelligence:** Debessonet/Cross 1:2, Gruner 1:2
- **AT&T consent decree:** Sullivan/Hertz 5:2
- **Atari:** Lunney 5:1

B

- **Baby Bells:** Sullivan/Hertz 5:2
- **bioengineered food:** Herman 7:1
- **biological deposit requirement:** Weitz 8:2
- **biological material transfers:** Rowland 1:1
- **biomedical ethics:** Meeker 9:2, Reisman 10:2, Rosenkranz 2:1
- **biotechnology (see also genetic engineering)**
 - **generally:** Ausubel 4:1, Hasan 9:2, Herman 7:1, Johnston 4:2, Maatz 7:1, Naumann 1:1, Rowland 1:1, Traynor/Cunningham 3:2, Weitz 8:2
 - **food:** Herman 7:1
 - **physician-researcher:** Maatz 7:1
 - **product liability:** Fox/Traynor 6:1, Stovsky 6:2
 - **regulation:** Herman 7:1

C

- **CPUC:** Manheim 2:1
- **California Public Utilities Commission:** Manheim 2:1
- **causation:** Poulter 7:2
- **cell-line:** Dorney 5:2
- **chemical industry:** Hasan 9:2
- **Clipper scheme:** Koffsky 9:1
- **closed system:** Lunney 5:1
- **colorization:** McNally 5:1
- **Comment "k":** Fox/Traynor 6:1

- **computer animation:** Beard 8:1, Selbak 9:2, Sullivan 3:2
- **computer-generated re-enactments:** Sullivan 3:2
- **computer hardware**
 - **chip piracy:** Kasch 7:1
 - **copyright (see also copyright):** Nicholson 10:1
 - **reverse engineering:** Kasch 7:1
 - **Semiconductor Chip Protection Act of 1984:** Kasch 7:1
- **computer research:** Berring 1:1
- **computer security:** Rustad/Eisenschmidt 10:2
- **computer software**
 - **generally:** Burgunder/Heckman 2:2, Feldman 9:1, Kuo 2:1, Lunney 5:1, Pinheiro/Lacroix 1:2, Samuelson 6:2
 - **behavior:** Carleton 10:2
 - **copyright (see also copyright):** Barkan 7:2, Burgunder/Heckman 2:2, Carleton 10:2, Lemley 10:1, Loewenheim 4:2, McManis 8:1, Nicholson 10:1, Pinheiro/Lacroix 1:2, Rosler 10:1, Samuelson 6:2, Stork 3:2, Wrenn 4:2
 - **European Community Directive:** McManis 8:1
 - **networks:** Rustad/Eisenschmidt 10:2
 - **Object-Oriented Programming:** Barkan 7:2
 - **patent:** Barkan 7:2
 - **product liability (see also product liability):** Gill 1:2, Levy/Bell 5:1
 - **reverse engineering:** McManis 8:1
 - **user interfaces:** Samuelson 6:2
 - **vendors:** Levy/Bell 5:1
- **computer systems:** Debessonet/Cross 1:2, Gruner 1:2
- **conceptual retrieval:** Debessonet/Cross 1:2
- **confidentiality:** Feldman 9:1
- **conflict of interest**
 - **physician-researcher:** Maatz 7:1
 - **informed consent:** Maatz 7:1
- **constitutional law (see also First Amendment, Fourth Amendment):** Robinson 3:1
- **contract law:** Rowland 1:1
- **contract liability:** Levy/Bell 5:1
- **Cooperative Research Act of 1984:** Wright 1:1
- **copyright**
 - **generally:** Jones 1:2, Loewenheim 4:2, Paepke 2:1, Stork 3:2, Wrenn 4:2
 - **abstraction-filtration comparison test:** Lemley 10:1
 - **Act of 1976, Section 102(b) of:** Samuelson 6:2
 - **biotechnology:** Hogle 5:1
 - **computer animation:** Beard 8:1
 - **computer hardware:** Nicholson 10:1
 - **computer software (see also computer software):** Barkan 7:2, Burgunder/Heckman 2:2, Carleton 10:2, Loewenheim

- 4:2, McManis 8:1, Nicholson 10:1, Rosler 10:1, Pinheiro/Lacroix 1:2, Samuelson 6:2, Stork 3:2, Wrenn 4:2
- **fair use:** McManis 8:1, Seecof 5:2
- **misuse:** McManis 8:1, Paredes 9:2
- **Object-Oriented Programming:** Barkan 7:2
- **corporate venue:** Rich 5:2
- **credit law:** Nimmer/Krauthaus 2:2

D

- **database:** Rosler 10:1
- **digital manipulation:** Beard 8:1, Seecof 5:2
- **disclosure requirement:** Weitz 8:2
- **doctrine of equivalents:** Douros 10:2, Kushan 6:1, Thomas 10:1
- **duty to defend:** Cabot 8:2
- **duty to rescue:** Rosenkranz 2:1

E

- **EPA:** McGarity 9:1
- **e-mail (see electronic mail)**
- **economics of patent law:** Merges 7:1
- **electricity:** Manheim 2:1
- **electronic mail**
 - **business:** Winters 8:1
 - **employee rights:** Winters 8:1
 - **privacy rights:** Winters 8:1
- **electronic surveillance:** Koffsky 9:1
- **employment**
 - **electronic mail:** Winters 8:1
 - **law generally:** Feldman 9:1
 - **privacy rights:** Winters 8:1
- **energy:** Manheim 2:1
- **enhanced service providers:** May/Whitt 8:1
- **encryption:** Koffsky 9:1
- **environmental law:** Ausubel 4:1, Robinson 3:1
- **Environmental Protection Agency (EPA):** McGarity 9:1
- **equal protection:** Yin 8:2
- **equitable patent protection:** Kushan 6:1
- **equivalents, doctrine of:** Douros 10:2 ; Kushan 6:1; Thomas 10:1
- **ethics**
 - **biomedical:** Meeker 9:2, Reisman 10:2, Rosenkranz 2:1
 - **engineering:** Pace 9:1
 - **legal:** Pace 9:1
- **European Community Directive on Software Reverse Engineering:** McManis 8:1, Rosler 10:1
- **evidence:** Johnston 2:2, Selbak 9:2, Sullivan 3:2
- **excised tissue:** Dorney 5:2, Meeker 9:2

- expert systems
 - legal: Gruner 1:2
 - medical: Gill 1:2
- expert testimony: Johnston 2:2, Poulter 7:2, Selbak 9:2
- experimental use exception: Michel 7:2
- exports: Zschau 1:1

F

- FCC: Darr 6:1, May/Whitt 8:1
- FDA: Ausubel 4:1
- FERC: Manheim 2:1
- fact finding
 - legal: Denmark 8:2
 - scientific: Denmark 8:2
- fair use
 - generally: Seecof 5:2
 - computer animation: Beard 8:1
 - computer software: McManis 8:1
 - reverse engineering: McManis 8:1
- Federal Communications Commission (FCC): Darr 6:1, May/Whitt 8:1
- Federal Department of Agriculture (FDA): Ausubel 4:1
- Federal Energy Regulatory Commission (FERC): Manheim 2:1
- federal funding: McGarity 9:1
- federal grants: McGarity 9:1
- Federal Rules of Evidence: Selbak 9:2
- film: Beard 8:1, McNally 5:1
- finance law: Nimmer/Krauthaus 2:2
- First Amendment: Merges/Reynolds 3:1, Yin 8:2
- food, bioengineered: Herman 7:1
- Food and Drug Administration (FDA): Ausubel 4:1
- Fourth Amendment: Koffsky 9:1, Steele 6:2
- free-rider problem: Paepke 2:1
- free trade: Brooks 6:1
- freedom of the press: Yin 8:2

G

- General Agreement on Tariffs and Trade (GATT): Brooks 6:1
- genetic engineering (see also biotechnology)
 - generally: Ausubel 4:1, Johnston 4:2, Naumann 1:1, Rosenkranz 2:1, Traynor/Cunningham 3:2
 - food: Herman 7:1

H

- Hand formula: Douros 10:2

- hardware (see computer hardware)
- high technology innovation (see also industrial policy): Jorde/Teece 4:1, Thomas 10:1
- human tissue: Dorney 5:2, Meeker 9:2

I

- IVF: Martin/Lagod 5:2, Meeker 9:2
- image processing: Seecof 5:2
- in vitro fertilization (IVF): Martin/Lagod 5:2, Meeker 9:2
- inducement: Cabot 8:2
- industrial policy: Jorde/Teece 4:1, May/Whitt 8:1
- information services: May/Whitt 8:1
- information technology: Nimmer/Krauthaus 2:2
- informed consent: Dorney 5:2, Maatz 7:1
- insurance: Cabot 8:2
- intellectual property: Burgunder/Heckman 2:2, Kuo 2:1, Nimmer/Krauthaus 2:2, Rowland 1:1, Samuelson 6:2
- international trade: Zschau 1:1
- Internet: Rustad/Eisenschmidt 10:2

J

- joint ventures: Stockdale 7:2, Wright 1:1
- Judicial Improvements and Access to Justice Act: Rich 5:2
- junk science: Poulter 7:2

KL

- legal expert systems: Gruner 1:2
- legal research: Berring 1:1
- licensing: Lunney 5:1, Rustad/Eisenschmidt 10:2
- litigation: Wrenn 4:2
- lock-out chip: Lunney 5:1
- look and feel: Burgunder/Heckman 2:2, Carleton 10:2; Pinheiro/Lacroix 1:2, Samuelson 6:2;

M

- medical expert systems: Gill 1:2
- military space technology (see also space law): Johnson 3:1
- missile technology control regime: Hurewitz 9:2
- misuse: McManis 8:1, Paredes 9:2
- misappropriation: Paepke 2:1
- monopoly: Lunney 5:1
- motions to remand: Rich 5:2

N

- **NCRA:** Lee/Lee 6:2
- **NEA:** McGarity 9:1
- **NFPA:** McNally 5:1
- **NIH:** McGarity 9:1
- **NSF:** McGarity 9:1
- **National Cooperative Research Act (NCRA):** Lee/Lee 6:2
- **National Endowment for the Arts (NEA):** McGarity 9:1
- **National Film Preservation Act (NFPA):** McNally 5:1
- **National Institutes of Health (NIH):** McGarity 9:1
- **National Science Foundation (NSF):** McGarity 9:1
- **national security:** Zschau 1:1
- **negligence:** Fox/Traynor 6:1, Stovsky 6:2
- **Nintendo:** Lunney 5:1

O

- **object-oriented programming:** Barkan 7:2
- **obviousness:** Merges 7:1
- **on-line services:** Yin 8:2
- **open fields doctrine:** Steele 6:2
- **Outer Space Treaty:** Hurewitz 9:2

P

- **PCS:** Larson/Schroepfer 6:2
- **PURPA:** Manheim 2:1
- **parent/child relationship**
- **Particularity Clause:** Koffsky 9:1
- **patent law**
 - **generally:** Cabot 8:2, Hasan 9:2, Johnston 4:2, Loewenheim 4:2, Paepke 2:1, Weitz 8:2, Wrenn 4:2
 - **biological deposit requirement:** Weitz 8:2
 - **computer software:** Barkan 7:2
 - **disclosure requirement:** Weitz 8:2
 - **doctrine of equivalents:** Douros 10:2, Kushan 6:1, Thomas 10:1
 - **economic analysis:** Merges 7:1
 - **equitable patent protection:** Kushan 6:1
 - **experimental use exception:** Michel 7:2
 - **Hand formula applied to:** Douros 10:2
 - **medical techniques:** Reisman 10:2
 - **object-oriented programming:** Barkan 7:2
 - **obviousness:** Merges 7:1
 - **patent infringement:** Cabot 8:2
 - **inducement:** Cabot 8:2
 - **protein:** Kushan 6:1
 - **surgical techniques:** Reisman 10:2

- uncertainty: Merges 7:1
- utility requirement: Hasan 9:2
- peer review: McGarity 9:1
- **Personal Communication Services (PCS):** Larson/Schroepfer 6:2
- physician-researcher: Maatz 7:1
- power: Manheim 2:1
- preembryo: Martin/Lagod 5:2
- preembryonic research: Martin/Lagod 5:2
- preemption: McManis 8:1
- privacy: Winters 8:1
- product liability: Fox/Traynor 6:1, Gill 1:2, Levy/Bell 5:1, Stovsky 6:2, Traynor/Cunningham 3:2
- production joint ventures: Stockdale 7:2
- property rights
 - generally: Jones 1:2, Rowland 1:1
 - in human body: Dorney 5:2
- proprietary information: Feldman 9:1
- protein patents and technology: Kushan 6:1
- public utilities: Manheim 2:1
- **Public Utilities Regulatory Policy Act of 1978 (PURPA):** Manheim 2:1

QR

- radio spectrum allocation: Larson/Schroepfer 6:2
- **Regional Bell Operating Companies (RBOCs):** Sullivan/Hertz 5:2
- reanimation: Beard 8:1
- regulation
 - generally: Sullivan/Hertz 5:2
 - bioengineered food: Herman 7:1
 - genetic engineering: Naumann 1:1
 - telephone: Darr 6:1, May/Whitt 8:1
- removal procedures: Rich 5:2
- reproductive rights: Martin/Lagod 5:2
- reproductive technologies: Martin/Lagod 5:2, Meeker 9:2
- research / research and development
 - antitrust law: Stockdale 7:2
 - computer: Berring 1:1
 - conflict of interest: Maatz 7:1
 - cooperation (see also research - joint ventures): Lee/Lee 6:2
 - effect of patentability on: Merges 7:1
 - experimental use exception: Michel 7:2
 - federally funded: Michel 7:2
 - industry funded: Maatz 7:1
 - joint ventures (see also research - cooperation): Stockdale 7:2

- legal: Berring 1:1
- reverse engineering
 - chips: Kasch 7:1
 - computer software: McManis 8:1
 - fair use: McManis 8:1
 - misuse: McManis 8:1

S

- satellite
 - imagery: Steele 6:2
 - launching services: Brooks 6:1
 - media and technology: Merges/Reynolds 3:1
 - remote sensing technology: Steele 6:2
- scanning: Seecof 5:2
- scientific evidence: Poulter 7:2, Selbak 9:2
- scientific research data: Jones 1:2
- search and seizure: Koffsky 9:1
- Semiconductor Chip Protection Act of 1984: Kasch 7:1
- software (see computer software)
- space law and policy: Brooks 6:1, Danilenko 4:2, Fought 3:1, Hurewitz 9:2, Johnson 3:1, Merges/Reynolds 3:1, Robinson 3:1
- state of the art defense (see also product liability): Stovsky 6:2
- statutory interpretation: Debessonnet/Cross 1:2
- still image processing: Seecof 5:2
- strict liability (see also product liability): Fox/Traynor 6:1, Stovsky 6:2

T

- tangible/intangible property: Kuo 2:1
- taxation: Kuo 2:1
- technology consortia: Lee/Lee 6:2
- telecommunications (see also telephone)
 - generally: Darr 6:1, Sullivan/Hertz 5:2
 - regulation of: Larson/Schroepfer 6:2
- telephone (see also telecommunications)
 - alternative operator services: Darr 6:1
 - enhanced service providers: May/Whitt 8:1
 - Federal Communications Commission: Darr 6:1, May/Whitt 8:1
 - industrial policy: May/Whitt 8:1
 - information services: May/Whitt 8:1
 - rate structures: May/Whitt 8:1
- tort liability: Fox/Traynor 6:1, Levy/Bell 5:1, Paepke 2:1, Poulter 7:2
- toxic torts: Poulter 7:2
- trade secret law: Feldman 9:1, Nicholson 10:1, Paepke 2:1

- **trademark law:** Loewenheim 4:2, Wrenn 4:2
- **tying:** Paredes 9:2

U

- **UAGA:** Dorney 5:2
- **unavoidably unsafe products defense (see also product liability):** Stovsky 6:2
- **uncertainty standard of patentability:** Merges 7:1
- **unfair competition:** Cabot 8:2, Loewenheim 4:2
- **Uniform Anatomical Gift Act (UAGA):** Dorney 5:2
- **Uniform Commercial Code (UCC):** Rustad/Eisenschmidt 10:2
- **university research**
 - **conflict of interest:** Maatz 7:1
 - **experimental use exception:** Michel 7:2
 - **informed consent:** Maatz 7:1
- **user interfaces, computer software:** Samuelson 6:2

V

- **venue:** Rich 5:2
- **video game:** Lunney 5:1

WXYZ

- **wireless communication:** Larson/Schroepfer 6:2
- **wiretap:** Koffsky 9:1
- **x-ray crystallography:** Hogle 5:1

TITLE INDEX

A

- *AT&T Antitrust Consent Decree: Should Congress Change the Rules?, The*, Lawrence A. Sullivan and Ellen Hertz, Issue 5:2 (Fall 1990)
- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost?*, Donald Stockdale, Issue 7:2 (Fall 1992)
- *Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information, An*, Cary Debessonnet and George Cross, Issue 1:2 (Fall 1986)
- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Glynn Lunney, Issue 5:1 (Spring 1990)

B

- *Behavior-Based Model for Determining Software Copyright Infringement*, A, Dennis M. Carleton, Issue 10:2 (Fall 1995)
- *Biological Deposit Requirement: A Means of Assuring Adequate Disclosure, The*, David Weitz, Issue 8:2 (Fall 1993)
- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Eleanor Fox and Michael Traynor, Issue 6:1 (Spring 1991)

C

- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Joseph Beard, Issue 8:1 (Spring 1993)
 - *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Mark Koffsky, Issue 9:1 (Spring 1994)
 - *Commercial Law of Internet Security, The*, Michael Rustad and Lori E. Eisenschmidt, Issue 10:2 (Fall 1995)
 - *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Pamela Samuelson, Issue 6:2 (Fall 1991)
-

- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Barry Sullivan, Issue 3:2 (Fall 1988)
- *Computerized Citation Checking Revisited*, Mark Welch and Barry Bayer, Issue 3:2 (Fall 1988)
- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Janine McNally, Issue 5:1 (Spring 1990)
- *Convergence in the Law of Software Copyright?*, Mark A. Lemley, Issue 10:1 (Spring 1995)
- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?*, Troy Paredes, Issue 9:2 (Fall 1994)
- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Doreen Hogle, Issue 5:1 (Spring 1990)
- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Pamela Johnston, Issue 2:2 (Fall 1987)
- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, E. Joshua Rosenkranz, Issue 2:1 (Spring 1987)

D

- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, John Selbak, Issue 9:2 (Fall 1994)

E

- *Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, An, C. Owen Paepke, Issue 2:1 (Spring 1987)
- *Emerging Product Liability Issues in Biotechnology*, Michael Traynor and Brian Cunningham, Issue 3:2 (Fall 1988)
- *Emerging Theory of Computer Software Genericism*, An, Lee Burgunder and Carey Heckman, Issue 2:2 (Fall 1987)
- *European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, The, Debra B. Rosler, Issue 10:1 (Spring 1995)
- *Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, The, Suzanne Michel, Issue 7:2 (Fall 1992)
- *Export Controls and America's Competitive Challenge*, Ed Zschau, Issue 1:1 (Spring 1986)

F

- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Gregory Wrenn, Issue 4:2 (Fall 1989)
- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Warren Ausubel, Issue 4:1 (Spring 1989)
- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Adrienne Naumann, Issue 1:1 (Spring 1986)
- *Full-Text Databases and Legal Research: Backing Into the Future*, Robert Berring, Issue 1:1 (Spring 1986)

G

- *Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM, The*, Bradley J. Nicholson, Issue 10:1 (Spring 1995)

H

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Mavis Lee and Michele Lee, Issue 6:2 (Fall 1991)
- *Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research, The*, Patricia Martin and Martin Lagod, Issue 5:2 (Fall 1990)

I

- *Impact of International Law and Treaty Obligations on United States Military Activities in Space, The*, Dana Johnson, Issue 3:1 (Spring 1988)
- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Randolph May and Richard Whitt, Issue 8:1 (Spring 1993)
- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Thomas Jorde and David Teece, Issue 4:1 (Spring 1989)
- *Intellectual Property Law and the Venture Capitalist Process*, Alexander Silverman, Issue 5:1 (Spring 1990)
- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Charles McManis, Issue 8:1 (Spring 1993)

- *Is There a Property Interest in Scientific Research Data?*, Richard Jones, Issue 1:2 (Fall 1986)
- *Issues in the Regulation of Bioengineered Food*, Karen Goldman Herman, Issue 7:1 (Spring 1992)
- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Heather J. Meeker, Issue 9:2 (Fall 1994)

J

- *Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More, The*, Allen Rich, Gaynell Methvin and Thomas Crisman, Issue 5:2 (Fall 1990)

KL

- *Legal Aspects of the Commercialization of Space Transportation Systems*, Bonnie Fought, Issue 3:1 (Spring 1988)
- *Legal Implications of Letter Licenses for Biotechnology*, Bertram Rowland, Issue 1:1 (Spring 1986)
- *Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, The, Kimberly Pace, Issue 9:1 (Spring 1994)
- *Legal Protection for Computer Programs in West Germany*, Ulrich Loewenheim, Issue 4:2 (Fall 1989)
- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Timothy J. Douros, Issue 10:2 (Fall 1995)

M

- *Medical Expert Systems: Grappling with Issues of Liability*, Christopher Gill, Issue 1:2 (Fall 1986)
- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Maureen Dorney, Issue 5:2 (Fall 1990)

N

- *National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures, The*, Christopher Wright, Issue 1:1 (Spring 1986)
- *New Privacy Interest: Electronic Mail in the Workplace, The*, Steven Winters, Issue 8:1 (Spring 1993)

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Alexander Larson and Terrence Schroepfer, Issue 6:2 (Fall 1991)
- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Robert Merges and Glenn Reynolds, Issue 3:1 (Spring 1988)
- *Non-Proliferation and Free Access to Outer Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Barry J. Hurewitz, Issue 9:2 (Fall 1994)

O

- *Outer Space and the Multilateral Treaty-Making Process*, Gennady Danilenko, Issue 4:2 (Fall 1989)

P

- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Sean Johnston, Issue 4:2 (Fall 1989)
- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Thomas McGarity, Issue 9:1 (Spring 1994)
- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Joseph M. Reisman, Issue 10:2 (Fall 1995)
- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Tung Yin, Issue 8:2 (Fall 1993)
- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Michael Stovsky, Issue 6:2 (Fall 1991)
- *Protecting the "Look and Feel" of Computer Software*, John Pinheiro and Gerard Lacroix, Issue 1:2 (Fall 1986)
- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Jeffrey Kushan, Issue 6:1 (Spring 1991)

Q

- *Question Concerning Patent Law and Pioneer Inventions, The*, John R. Thomas, Issue 10:1 (Spring 1995)

R

- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, George Robinson, Issue 3:1 (Spring 1988)
- *Regulating International Trade in Launch Services*, Timothy Brooks, Issue 6:1 (Spring 1991)
- *Regulation of Alternative Operator Services*, Frank Darr, Issue 6:1 (Spring 1991)

S

- *Sales/Use Taxation of Software: An Issue of Tangibility*, John Kuo, Issue 2:1 (Spring 1987)
- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Benjamin Seecof, Issue 5:2 (Fall 1990)
- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Susan Poulter, Issue 7:2 (Fall 1992)
- *Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth,"* The, Howard Denmark, Issue 8:2 (Fall 1993)
- *Secured Financing and Information Property Rights*, Raymond Nimmer and Patricia Krauthaus, Issue 2:2 (Fall 1987)
- *Semiconductor Chip Protection Act: Past, Present, and Future*, The, Steven Kasch, Issue 7:1 (Spring 1992)
- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, David Barkan, Issue 7:2 (Fall 1992)
- *Software Product Liability: Understanding and Minimizing the Risks*, Lawrence Levy and Suzanne Bell, Issue 5:1 (Spring 1990)
- *Sound Sampling Protection and Infringement in Today's Music Industry*, Molly McGraw, Issue 4:1 (Spring 1989)

T

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Richard Gruner, Issue 1:2 (Fall 1986)
- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Miles Feldman, Issue 9:1 (Spring 1994)

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, William Manheim, Issue 2:1 (Spring 1987)

U

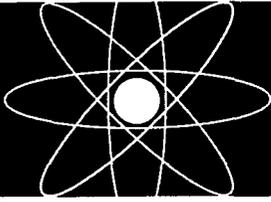
- *Uncertainty and the Standard of Patentability*, Robert Merges, Issue 7:1 (Spring 1992)
- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Claire Turcotte Maatz, Issue 7:1 (Spring 1992)
- *Use of Arbitration in Copyright Disputes: IBM v. Fujitsu, The*, Anita Stork, Issue 3:2 (Fall 1988)

V

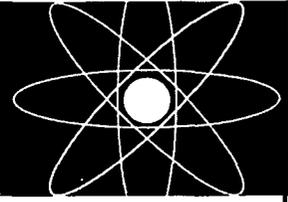
- *View From on High: Satellite Remote Sensing Technology and the Fourth Amendment, The*, Lisa Steele, Issue 6:2 (Fall 1991)

WXYZ

- *Watercloud Muddies the Water for Patent Coverage Disputes*, Howard Ross Cabot, Issue 8:2 (Fall 1993)



CALIFORNIA



ELEMENTS OF CONTROVERSY

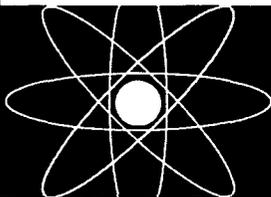
*The Atomic Energy Commission and
Radiation Safety in Nuclear Weapons
Testing, 1947-1974*

by **BARTON C. HACKER**

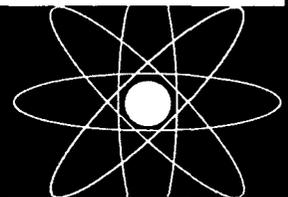
Despite these dramatic revelations important questions remain—the most controversial being: did the radiation overexposure in fact cause the cancers and birth defects for which it has been blamed? Hacker's work is the result of a decade of exhaustive research in AEC records and the full clinical and epidemiological literature on radiation effects. Although more concerned with uncovering the historical story than with assigning blame, the Department of Energy delayed publication of Hacker's study for five years.

Unforgettable congressional hearings in 1978 revealed that fallout from American nuclear weapons testing in the 1950s had overexposed hundreds of soldiers and other citizens to radiation. Faith in governmental integrity was shaken, and many people have assumed that such overexposure caused great damage.

\$55.00 cloth at bookstores or order toll-free 1-800-822-6657.



UNIVERSITY OF CALIFORNIA PRESS



CONTENTS

HIGH TECHNOLOGY LAW JOURNAL

VOLUME 10 NUMBER 2 1995

ARTICLES

The Commercial Law of Internet Security

Michael Rustad and Lori E. Eisenschmidt 213

Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents

Timothy J. Douros 321

COMMENTS

Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics

Joseph M. Reisman 355

A Behavior-Based Model for Determining Software Copyright Infringement

Dennis M. Carleton 405

BOOK REVIEW

DNA in the Courtroom: A Trial Watcher's Guide by Howard C. Coleman and Eric D. Swenson

Reviewed by Jasmine Samrad 433

INDEXES

Author Index 447

Issue Index 460

Subject Index 466

Title Index 475

ARTICLE

THE COMMERCIAL LAW OF INTERNET SECURITY

MICHAEL RUSTAD[†] AND LORI E. EISENSCHMIDT^{††}

TABLE OF CONTENTS

I.	INTRODUCTION	214
II.	STATE-OF-THE-ART NETWORK SECURITY.....	218
	A. The Technical Elements of Network Security	220
	B. The Internet/Network Security Industry.....	239

© 1995 Michael Rustad & Lori E. Eisenschmidt.

[†] Professor of Law, Suffolk University Law School; LL.M., 1986, Harvard University; J.D., 1984, Suffolk University Law School; Ph.D., 1981, Boston College. Prof. Rustad teaches courses in commercial law, torts and high technology law. He is a member of the American Law Institute and a Task Leader of the ABA Business Law Section's Subcommittee on Software Contracting. He is Co-Chair of the Task Force on General Provisions of the Proposed U.C.C. Article 2B on the licensing of intangibles.

^{††} J.D. Candidate, 1996, Suffolk University Law School; B.A., 1985, University of South Florida. Ms. Eisenschmidt co-authored working papers on tort law and security with Professor Rustad for the ABA Science and Technology Section's Law and Ethics on the 'Nets project ("Project LEON") in the Spring of 1995.

The authors gratefully acknowledge the exhaustive technical consultation and review provided by Harold H. Leach, Jr., J.D., LL.M. Mr. Leach is a principal in the Boston-based computer consulting firm Legal Computer Solutions, Inc. His firm specializes in automating law firms and legal departments. Mr. Leach was formerly a partner at the Boston law firm of Choate, Hall & Stewart. The authors would like to thank Professor Jeffrey Atik of Suffolk University Law School and Ellen Kirsh, Vice President and General Counsel of America Online, Inc., for providing materials and valuable suggestions. We would also like to thank Barry Nelson, a former BBN systems engineer and current third-year student at Suffolk University Law School, for his critical reading and editorial assistance. Fourth-year evening students Charles Rosenthal and Elaine Martel were instrumental in the design and execution of the Computer Law Association Survey. The valuable research assistance of Kizuki Kuzuhari, F.A. Lichauco and Chris Palmisano should also be acknowledged. We would also like to thank the reference librarians of Suffolk University Law School. Finally, our thanks and appreciation are extended to Sylvia Michaud for unflagging administrative assistance. The opinions expressed in this paper should not be attributed to our colleagues or institutions.

III. THE QUESTION OF LEGAL STANDARDS FOR INTERNET SECURITY	243
A. Regulation Under Tort Law	244
B. Regulation Under Current Contract Law	262
IV. REGULATION OF INTERNET SECURITY PRODUCTS UNDER PROPOSED U.C.C. ARTICLE 2B.....	274
A. Anatomy of Proposed U.C.C. Article 2B	278
B. The Case for Adopting the Proposed Article 2B for Internet Security Software.....	293
V. CONCLUSION	300
VI. APPENDIX A: EXAMPLE OF SALES AND LICENSE AGREEMENT OF A NETWORK SECURITY PRODUCT	302
VII. APPENDIX B: COMPUTER LAW ASSOCIATION SURVEY AND RESULTS.....	313

I would not want to depend on the Internet for the livelihood of my business The reality is that Internet security is basically an oxymoron.¹

Security on the Internet is a solved issue. By year's end, off-the-shelf products will be available to ensure secure Internet transactions.²

I. INTRODUCTION

Since the Clinton administration endorsed the establishment of a National Information Infrastructure (NII),³ the rise in Internet use has been meteoric. As of July 1995, the Internet links an estimated thirty million users, and the number of users continues to grow an astonishing 20% per month.⁴ In the past decade, the Internet has grown from

1. Laurent Belsie, *Computer Theft Cases Show Holes in Internet*, CHRISTIAN SCIENCE MONITOR, Mar. 1, 1995, at 3 (quoting Daniel White, Partner, Ernst & Young).

2. Peggy Liu, Product Manager, NetManage, Inc., Presentation at 1995 Spring Workshop: Internet and the Entrepreneur, MIT Enterprise Forum of Cambridge, Inc. (Apr. 22, 1995).

3. John Byczkowski, *U.S. Grappling with Access to Information*, CINCINNATI ENQUIRER, Mar. 7, 1995, at B06; Calvin Reid, *Publishers Support Clinton Report on Copyright, Cyberspace. 'Intellectual Property and the National Information Infrastructure' Report Recommends Limited Amendments to the Copyright Act to Properly Protect New Technologies*, 242 PUBLISHERS WKLY. 11 (Sept. 11, 1995).

4. April Streeter, *Don't Get Burned By the Internet*, LAN TIMES, Feb. 13, 1995, at 58 (quoting 20% growth figure provided by the Carnegie Mellon University Computer Emergency Response Team); Arthur Middleton Hughes, *Internet DB Marketing with*

1,000 end-user computers to greater than two million.⁵ The development of the World Wide Web (WWW or Web), an increasingly interactive medium supporting high-resolution color graphics and multimedia presentations, has fueled this growth. Of the already thirty million Internet users, a minimum of fifteen million have access to the World Wide Web.⁶ The Web is projected to have just under twenty-two million users by the turn of the century.⁷

In addition to individuals, large and small corporations, law firms and legal departments, and specialty boutiques and consultant service providers are discovering the power of the Internet. Advances in technology and user-friendly access have made it more desirable and economically feasible to connect parent and subsidiary corporations through the Internet instead of through more expensive private networks. Strategic business alliances are using the Internet for global networking and data transfers. Even advertising is finding a niche—the cost of advertising on the Web is “minuscule” relative to that of advertising in a newspaper, and advertisers have access to millions of Internet users.⁸

Amidst the surging excitement and interest, however, runs a deep thread of ambivalence toward connecting to the Internet. The Internet’s evil twin is the home of “Bad Guys”—hackers,⁹ crackers, snackers, stalkers, phone phreaks and other creepy Web crawlers.¹⁰ Businesses fear that the Infobahn could suddenly veer into the highway to Hell.¹¹ Insincere and downright devious transactions by malefactors may cause a firm to unwittingly disclose its prime

CD-ROMs, *DM NEWS*, Aug. 21, 1995, at 22 (stating that the network consists of “almost five million” server computers).

5. Richard Raysman & Peter Brown, *On-Line Legal Issues*, N.Y. L.J., Feb. 15, 1995, at 30.

6. Hughes, *supra* note 4, at 1.

7. Belsie, *supra* note 1, at 3 (quoting Forrester Research, Inc.).

8. Arnold Kling, *Mortgages over the Internet*, 55 *MORTGAGE BANKING* 18 (Nov. 1994); *CompuServe*, *NMAA Sign Multimillion-Dollar Internet Access Agreement; NMAA Members Offered Free Internet Test-Drive*, *PR NEWSWIRE*, Aug. 21, 1995.

9. This article uses “hacker” to encompass any malevolent intruders. Historically, however, it should be understood that the term “hacker,” “coined at MIT in the 1960s, simply connoted a computer virtuoso.” Wade Roush, *Hackers: Taking a Byte Out of Computer Crime*, *TECH. REV.*, Apr. 1995, at 32. Internet cultural anthropologists distinguish between crackers, snackers and hackers. Technically, “crackers” thrive on the challenges of breaking in, “snackers” try to see what is interesting, and “hackers” intrude for the intellectual curiosity of understanding how things work.

10. Maggie Cannon, *Life in the Big City: Internet Concerns*, *MACUSER*, May 1995, at 17 (describing creepy characters residing on the Infobahn).

11. Internet deviants have captured the imagination of mass culture. For example, Fox Television Network has a new series featuring a New York City undercover cop who tracks an Internet stalker. *ENTERTAINMENT WKLY.*, Sept. 15, 1995, at 73.

information commodities. Bad Guys could enter a firm's computer through the Internet connection and steal or compromise a firm's informational crown jewels.¹² Valuable information includes not only a company's marketable information products such as software, but also proprietary information such as customer lists, product designs, marketing plans and other trade secrets. Since this information is increasingly entrusted to, circulated on and stored in computer systems,¹³ the critical question is: "Just how secure is the Internet?"

Examples of hacker malfeasance and Internet insecurity are legion.¹⁴ A recent electronic bulletin board service survey reported that 69% of the respondents' firms perceived significant security threats.¹⁵ Half of those respondents reported theft of property of \$10,000 or more.¹⁶ Around 18% of the respondents reported that their firm was victimized by fraudulent computer activity by a trusted party or insider.¹⁷ Approximately 10% reported fraudulent losses to outsiders.¹⁸ About 93% of the responding firms had implemented a network security project.¹⁹

One Internet user purportedly set up an anonymous file-transfer protocol²⁰ (FTP) site called "INFES-Station BBS" that was allegedly intended to distribute virus code.²¹ Another hacker reportedly stole a number of sophisticated computer programs which may be used to unscramble cellular-telephone codes and to facilitate infiltration of

12. See David Bernstein, *Insulate Against Internet Intruders*, DATAMATION, Oct. 1, 1994, at 49.

13. Senator Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH. 1, 21 (1992) ("The maintenance of the security and integrity of computer systems has become increasingly critical to interstate and foreign commerce, communications, education, science, technology, and national security. As we move even further into the hi-tech age, we depend on computers to process essential information and to store it in a manner in which it will not be altered.").

14. One security expert finds scavenging, leakage, piggybacking, wire tapping, data diddling, viruses and salami-type thefts to be quite common. See generally RICHARD H. BAKER, NETWORK SECURITY: HOW TO PLAN FOR IT & HOW TO ACHIEVE IT 183 (1995).

15. *Id.* at 183-84 (reporting survey of COMSEC BBS).

16. *Id.* at 184.

17. *Id.*

18. *Id.*

19. *Id.*

20. Protocols are electronic communications "rules" which allow for the orderly, reliable transfer of data. A file-transfer protocol permits transfers of files between computers with unique software and hardware configurations. Other examples of protocols are the International Standards Organization (ISO) and the standard ASCII character set.

21. Gary H. Anthes, *Internet Triggers Virus Debate, Security Measures; Providers Dispute Accountability for Virus Distribution*, COMPUTERWORLD, Feb. 27, 1995, at 66.

other computers.²² Pentagon officials recently disclosed that, in a 1994 internal audit of their network security, an in-house team employing hacker techniques successfully penetrated 88% of the 8,900 government computers they attacked, with only 4% of the break-ins being detected.²³

Increased business activity on the Internet is likely attracting hacker activity.²⁴ Some malefactors hack business sites for the same reason Willie Sutton robbed banks: "That's where the money is."²⁵ Researchers at Carnegie Mellon University report that the increase in attempted intrusions to Internet hosts parallels the monthly rise in Internet connections.²⁶ By one estimate, the number of Internet break-ins has increased by more than 70% in each of the last two years.²⁷ Because of such security concerns, a December 1994 survey reported that many firms were deciding against connecting to the Internet.²⁸

The security risks of connecting to the Internet raise a number of legal questions not yet resolved by case law or commentary.²⁹ A large number of network security products has recently appeared on the market which claim to have solutions to the problem of the "Bad Internet."³⁰ One new security product was described as "close to the level of 'bullet-proof'."³¹ Some firms have even represented their

22. Michael Myer et al., *Stop! Cyberthief! Technology: Don't Be Alarmed, But the Law Can't Cope With Computer Crime*, NEWSWEEK, Feb. 6, 1995, at 36. These programs belonged to Tsutomu Shimomura and the San Diego Supercomputer Center. *Id.*

23. Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C03.

24. Streeter, *supra* note 4, at 58 (quoting Bill Pozerycki, Internet security service manager, Digital Equipment Corp., Maynard, Massachusetts).

25. This apocryphal statement should not be misconstrued as implying that the sole motivation behind all hacking is money. As explained in *supra* note 9, Internet cultural anthropologists differentiate among varying types of hackers according to their motivations.

26. Streeter, *supra* note 4, at 58.

27. Belsie, *supra* note 1, at 3.

28. *Internet World Investigates High Tech Security on the Internet*, BUSINESS WIRE, Dec. 19, 1994.

29. See generally I. Trotter Hardy, *The Proper Legal Regime for 'Cyberspace'*, 55 U. PITT. L. REV. 993, 994 (1994). See also Lawrence Lessig, *Symposium: Emerging Media Technology and the First Amendment: The Path of Cyberlaw*, 104 YALE L.J. 1743 (1995).

30. See Anne Knowles, *UUNet Suite Tightens Security: System Offers Firewall, Encryption for Virtual Private Networks*, PC WEEK, May 29, 1995, at 14; Erica Roberts, *Network Systems to Secure Hubs, Routers*, COMM. WEEK, Feb. 20, 1995, at 1 [hereinafter Roberts, *Network Systems*]; Erica Roberts, *Easing LAN Access to the Internet*, COMM. WEEK, Feb. 13, 1995, at 27; Streeter, *supra* note 4, at 58.

31. *Network Systems Offers Public, Private Network Data Security*, NETWORK MANAGEMENT SYSTEMS & STRATEGIES, Nov. 15, 1994, at 1043.

product(s) to be "hacker-proof."³² Because of the lag between the legal infrastructure and the new network security technologies, it is completely uncertain whether representations such as these would be deemed enforceable by a court of law.

This article examines a vital problem of the information technologies—the unresolved legal dilemmas arising out of the development of network security technologies. To understand the legal dilemmas raised by the new network security technologies, we first need an overview of how the technologies work. Part II of this article describes the components which comprise Internet security and reviews the state-of-the-art security devices and methods available to combat Internet abuse. It then reviews the spectrum of security products and the emerging network security industry.

Part III identifies the plight of courts, policy makers and vendors and vendees by setting forth key legal issues that arise out of these new technologies. Failure to resolve these legal dilemmas would result in the delay of the development of network security products serving the NII and the NII itself. Part III also provides a discussion of traditional tort and contract law, plus Article 2 of the Uniform Commercial Code (U.C.C.), as they might be applied to resolve these issues.

Part IV advocates the forthcoming licensing article (Article 2B) of the U.C.C. as a legal framework ideally suited for the resolution of the novel and complex issues posed by the marketing of Internet information security products. We contend that the emerging software licensing law is a flexible body of law adaptable for resolving numerous information technology issues. We assess the rules of the proposed Article 2B for providing a coherent legal framework for security network products. Since the proposed Article 2B alone cannot manage all liability concerns, we recognize a residual role for tort law for cases of market failure and for vindicating the rights of third parties injured by security breaches. Tort liability will also come into play if there is an independent tort arising out of a breach of contract. However, too much tort law may be detrimental to the continued development of the NII.

II. STATE-OF-THE-ART NETWORK SECURITY

"Network security" is much like home security. Precautions and safeguards are scaled to the level of risk. In a crime-free world, the

32. Roberts, *Network Systems*, *supra* note 30, at 1 (statement of Tom Gilbert, marketing director at Network Systems Corp.) ("We have comprehensive solutions . . . to provide hacker-proof security across any network.").

beginning and end of home security might be painting and weatherstripping the house—insulating against the elements and taking precautions to guard against fire and natural disasters. In such a neighborhood, intruder invasion is not a concern. The world, of course, is not a crime-free place, and neither is “Cyberspace.”³³ Just as products, devices and methods (such as locks, steel doors, security monitors and guards) have been developed and marketed to protect homes against unwarranted intrusion, an entire industry is arising to develop products and protocols designed to deter electronic invasion of computer systems.

Computer (or network) security differs from home security in two important respects. First, home security is primarily designed to prevent the theft of tangible items of property. In contrast, the network security industry must address the electronic, intangible nature of the computer data it seeks to protect. Even though the physical disks or diskettes used in connection with computers are tangible, the electronic data on them is a formless collection of magnetically-fixed electronic impulses. The network security industry’s objective is to protect this treasure trove of magnetic data from unwanted intrusion and theft. Were it not so, security for computers could be limited to physical harm and theft prevention, much like security for typewriters.

The second but related difference concerns the interconnectivity of computers. Unlike a home burglar, an intruder does not need to have *physical* access to a computer in order to effectuate an unauthorized entry; *electronic* access can suffice. Computers can be connected by wires, via modem and telephone lines, or even via the Internet. Once connected, computers and their precious data are potentially accessible to remote intruders, if appropriate security measures are not taken. This part lays out the basic principles underlying these inter-networking technologies, explores the various components of network security, and finally, discusses the role of the network security industry.

33. William Gibson coined the term “Cyberspace” in his 1984 science fiction book *Neuromancer* to describe the “virtual world created by a computer system.” Michael D. Scott, *Advertising in Cyberspace: Business and Legal Considerations*, COMPUTER LAWYER, Sept. 1995, at 1 n.1 (discussing WILLIAM GIBSON, *NEUROMANCER 2* (1984)). “Cyber” is derived from the Greek word “*kybernan*,” which means “to steer or control.” *Id.*

A. The Technical Elements of Network Security

1. CLIENT AND SERVER COMPUTERS

In order to develop a coherent legal regime for network security products, it is necessary to understand the basic principles underlying networking technologies. The degree of risk of Internet abuse depends on the method of Internet connectivity, the type of computer hardware used, the number and type of security devices in use, and the nature of the user (e.g., educational institution, government entity, business or home). In general, the risk factor is less for computers which access the Internet via an Internet service provider (ISP) than for computers which have direct access to the Internet. In addition, companies and governmental offices are most likely to be targeted by hackers, followed by educational institutions and homes.³⁴

The current trend is for businesses to link intracompany computers together by wire or cable to form a Local Area Network (LAN).³⁵ Software designed for a LAN permits linked computers to share programs and data files, and to exchange electronic mail (e-mail). It also permits shared printers, plotters, imaging devices, hard disks and other transfer and device concepts. The LAN comprises a mini-"data highway" with one of the computers acting as the resource manager or "server."³⁶

Any stand-alone IBM compatible personal computer (PC) or Macintosh computer (Mac) with a modem is an example of a simple "client" computer. The client computer typically connects to the Internet by establishing a telephone connection to an ISP computer. The ISP computer functions as a "server" computer, providing news and mail services, as well as routing data between the client computer and the rest of the Internet.³⁷ Server computers are connected by

34. Because government and business computer networks are more sophisticated and more closely guarded than home or school computer networks, hackers find the challenge of penetrating them more appealing. In addition, hackers seeking financial gain are more likely to reap substantial rewards from government or business computers than from home or school computers.

35. The rise of low-cost microcomputers in the 1980s facilitated the growth of LANs. IBM lost ground because of its failure to predict the decline of the mainframe computer and the rise of the LAN. Today, the desktop work station is the computer industry's *de facto* standard for software development.

36. The term "server" refers to any device which offers a service to network users.

37. ISPs with "dial-up" services are available in most cities. For example, in the Boston Metropolitan area, Internet connectivity services are available from North Shore Access of Lynn; Novalink of Westborough; and The Internet Access Co. of Bedford, to name a few. America Online, CompuServe and other commercial services have recently begun offering Internet access for use by their individual and business customers.

high-speed telephone lines to the network of computers which comprise the backbone of the Internet. The ISP's server computer is "on" the Internet twenty-four hours a day. Any computer "on" the Internet may be potentially "hacked into" from elsewhere on the Internet by the Bad Guys.

The popular wisdom is that a pure "client" computer or "client" computer network is a super-hero, easily able to keep out the Internet Bad Guys. It is shielded by an intermediary—the ISP server computer. Even if the ISP server is compromised, the client computer is still safe, because it lacks the communications protocols necessary to enable the hacker to establish a connection with it. Yet, if the client computer connects to the ISP computer via a Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) connection, it is likewise "on" the Internet and may be vulnerable to attack. This vulnerability, however, does not arise unless the client computer itself runs programs which allow it to act as a server.³⁸

The greatest threat to the security of client computers is not the Internet hacker, but rather the enemy within, the in-house hacker. Insiders who have high level computer-access privileges may abuse them. Insiders who have otherwise nominal access privileges can invade the computer system by "shoulder surfing," intercepting passwords of individuals with higher-level clearance. In this context, PC- and Mac-based LANs are more vulnerable to internal security breach than are mainframe computers: mainframe computer systems have traditionally had a department of Management Information Systems (MIS) dedicated to backups and security; no such tradition exists in the LAN environment.³⁹

2. ROUTERS/GATEWAYS

Many large companies and educational institutions equip their computers or LANs with "routers."⁴⁰ Routers allow them to access the Internet "directly," perhaps in combination with a gateway, rather than dialing-up and going through an ISP. Routers/gateways filter messages which are destined for recipients outside the local network.

38. Such a program is referred to in the industry as a "daemon-program."

39. *Network Help Desk*, NETWORK WORLD, Nov. 21, 1994, at 2.

40. A router is a device which employs special communications protocols. The protocols enable, at a minimum, the passing of information from the Internet to LAN destinations, and vice versa. A gateway may also be used if the LAN does not recognize Internet protocols such as System Network Architecture. The gateway performs the function of converting the disparate networks' protocols to the one compatible to its system. Additional protocols can be added to enable error detection and connection bookkeeping functions.

and receive messages from remote networks to be delivered locally on the LAN. Just as a group of computers in an office can be linked together to share files and e-mail through a LAN, LANs can themselves be networked on a world-wide scale. A multi-national corporation located in the Netherlands can thus be linked to its subsidiaries in England and South Africa via the Internet. Via the router/gateway, the companies' computers can send and receive electronic data and requests "directly" from the Internet.

It is important to note that companies and institutions connected to the Internet via a router/gateway are "on" the Internet, much like ISPs are directly on the Internet. They are thus at risk from Internet hackers. Because of this, if proper security precautions are not taken by the computer systems administrator (SysAdmin), the router/gateway may be the most vulnerable point in a company's network.

3. OPERATING SYSTEM

Security on the Internet is inseparable from the security of the computers that access and/or serve the Internet. At the server level, security can be breached on several fronts. The first vulnerability lies with the ISP hardware's operating system (O/S). The majority of the computers connecting the Internet use Unix-based or compatible standardized operating systems. Unix-based O/Ss were not originally designed with security in mind; they contain scores of well-known, documented security "loopholes." In addition, hackers occasionally discover new methods for circumventing supposedly secure aspects of the O/S.⁴¹ They may exploit such O/S weaknesses to gain some measure of unauthorized access and control.

For example, if a hacker penetrates an Internet service provider's O/S, he will be able to access at least some data stored on the ISP's computer. Depending on the severity of the loophole he has uncovered, he may be able to: access and copy a list of the server's accounts (i.e., the computers/companies which utilize that ISP to access the Internet); browse e-mail stored on the computer for some or all of the accounts; or disclose or damage ISP data files. In cases of severe breach, he can actually disrupt or halt the operation of the server's programs, and may be able to extend his destructiveness to other computers by introducing a malicious routine, such as a computer

41. The U.S. Government has funded the Computer Emergency Response Team (CERT) to track vulnerabilities and to warn SysAdmins to fix them. CERT issues security advisories which may be read on-line in the "comp.security.announce" newsgroup, or which may be sent directly to an individual or organization's e-mail account by subscribing to CERT's free mailing list.

"virus" or "worm."⁴² Worms and viruses are programmed to propagate their havoc automatically, ad infinitum.⁴³

Various means exist for ferreting out and plugging security holes at the O/S level.⁴⁴ SysAdmins can self-administer programming tools to search for vulnerabilities in their systems. Alternatively, a company may choose to hire a computer firm or consultant specializing in security to run the programs and/or perform a complete security analysis. Internet Security Systems, Inc. markets "Internet Scanner," purportedly the "most comprehensive 'attack simulator' available."⁴⁵ Its software "systematically probes an organization's network for security holes, providing a vulnerability report on each device on the network with recommendations for corrective action."⁴⁶ Internet Scanner scans for over 100 security vulnerabilities.⁴⁷

Other examples of diagnostics products include the controversial "Security Administrator Tool for Analyzing Networks" (SATAN) program, "COPS," "OmniGuard/Enterprise Access Control for Unix," and "NetProbe." SATAN's dual nature makes it controversial: because it functions by probing its target across the network from another host, it can be used to crack systems as well as to defend them.⁴⁸ Using SATAN, a hacker can systematically exploit any known system weakness which has not been remedied.⁴⁹ The other scanners run directly on the target host and operate as self-diagnostics.⁵⁰ SATAN and COPS can be downloaded from various servers on the Internet and used for free; the others are available

42. "Worm" and "virus" are defined as follows:

[A] "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.

United States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir.), cert denied, 502 U.S. 817 (1991).

43. John DeHaven, *State of the Art: Seeking Security Stealth Virus Attacks*, BYTE, May 1, 1993, at 137.

44. See generally ANDRE BACARD, *COMPUTER PRIVACY HANDBOOK* (1995); *IMPLEMENTING INTERNET SECURITY*. (Frederic J. Cooper et al., eds., 1995).

45. Thomas Noonan *Joins Internet Security Systems as President*, BUSINESS WIRE, Aug. 30, 1995.

46. *Id.*

47. *Id.*

48. Jason Levitt, *Techview: Dealing With the Devil*, INFORMATION WEEK, Apr. 17, 1995, at 42.

49. See Winn Schwartau, *The Key to Defeating SATAN is Understanding How It Can Bedevil You*, NETWORK WORLD, May 1, 1995, at 32.

50. Rkutrell Yasin, *Vendors Fire Up Wares to Vie with SATAN*, COMMUNICATIONS WEEK, Apr. 10, 1995, at 4.

commercially. Properly utilized, both types of products enable SysAdmins to find and plug O/S security holes before hackers can exploit them.

Since Unix-based O/Ss have numerous inherent security flaws, informal norms in the industry have filled the gaps. Some of the widely-shared industry practices include: monitoring for hacker programs,⁵¹ worms and viruses;⁵² blocking repetitive failed access attempts; maintaining adequate log-in and audit trail records,⁵³ and monitoring for other indicia of trouble. Now that extensive means are available to overcome the original security loopholes, operating system security is a "reasonable" proposition.⁵⁴

Other O/Ss, such as Digital Equipment Corporation's Open VMS/VAX 6.0 and Security Enhanced VAX/VMS, have been evaluated by the Department of Defense's National Computer Security Center (NCSC) and rated as meeting or exceeding security

51. One virulent hacker program permits the storage of a copy of a user's log-in for later retrieval and use by the hacker.

52. McAfee, which commands a 67% world-wide market share in virus detection products, offers "VirusScan" for non-Unix-based client and server computers. Its technology allows accurate detection of over 5,100 known and new viruses, including "boot viruses, file viruses, multi-partite viruses, stealth viruses, encrypted viruses, and polymorphic viruses." The company maintains a 24-hour Virus Emergency Response Center. *McAfee Releases VirusScan for Windows 95 and Announces Windows NT Support*, BUSINESS WIRE, Aug. 18, 1995. See also "<http://www.mcafee.com/a-v/pub/vscan.html>."

The leading European anti-virus software is "Dr. Solomon's Anti-Virus Toolkit," made by S&S Software International, Inc. It detects and "kills" more than 6,700 computer viruses. S&S Software International maintains a research team which detects 150 to 200 new viruses a month. The team provides 24- to 48-hour virus identification and also repair, if possible. The team has devised a downloadable program for Toolkit users for detecting the prolific new macro-based virus known variously as "WinWord.Concept," "WW6Macro," and "Prank Macro." They have also prepared a white paper with instructions on how to remove the virus. While specializing in security and networking products for IBM-compatible systems, S&S International is expected to release Macintosh, SCO UNIX, Windows 95, Windows NT Server and Windows NT Workstation versions of Toolkit in the fall of 1995. *New Computer Virus Infects Winword 6 Users; S&S Releases Fix for World's First Macro Virus*, PR NEWSWIRE, Aug. 30, 1995. See also "<http://www.drsolomon.com>."

53. Hackers' failed access attempts are often recorded on log on and audit trail records. The auditing function of security programs enables SysAdmins to track attempted break-ins. For example, in February of 1994, co-author Michael Rustad learned through an audit trail that an unknown hacker had attempted to break into his "punitive damages in products liability" database 134 times over a period of three days. Audit controls record every attempted log on and track who signs on when and to which files. Judith Silver, *Routine Workouts Keep VA Security Tight*, GOV'T COMPUTER NEWS, Aug. 8, 1994, at 71.

54. The other main tenet of network security, survivability/availability, is not addressed in this article. "Survivability" refers to the ability to maintain or restore hardware, software and data integrity in event of electronic or natural disaster. "Availability" refers to the consistency and continuity of network functioning.

specifications for C2⁵⁵ security classification.⁵⁶ However, these systems comprise only a small part of the Internet's backbone.

4. LOCAL AREA NETWORK

Network security may be compromised within a LAN. Readers will find words like "network," "computer system," and "LAN" used seemingly interchangeably with "Internet." Generally these terms have separate meanings. In the world of electronic-data security, however, they can be used to refer to computers potentially at risk from intrusion by other, remote computers by virtue of their interconnectedness. Obviously, if a computer or LAN has no connection to the Internet, it is not at risk from Internet hackers. Additionally, if a computer is simply a "stand-alone" computer—it has no connection to a LAN or modem or the Internet—it cannot be at risk from a remote computer. However, a computer connected to a LAN can potentially be hacked into remotely—by or from *any other computer connected to or able to connect to the LAN*. This is the essence of remote intrusion.

The most important protection measure is to restrict physical access to the LAN's server computer to trusted personnel to prevent potential in-house hacking. In addition, LAN O/Ss can be "secure" or "insecure," depending on their hardware, software and configuration. The government certifies federal agencies' operating systems as secure if they meet the standards for C2 security classification.⁵⁷ Currently,

55. The D to A1 rating system was designed by the NCSC, a division of the National Security Agency (NSA), based on a collection of 36 color-coded books known as the "Rainbow Series" (including the widely-referenced "Orange Book"). Under the 1987 Computer Security Act, C2 ("Controlled Access Protection") is the minimum rating federal agencies must comply with to protect sensitive but unclassified information. All hardware and software on the system, including security features, must periodically be tested to ensure proper functioning. Files can be shared, but file access must be controlled, and only authorized personnel may assign user rights. User identification and authentication is required, data must be protected from unauthorized users, and the computer system should protect itself from outside tampering. Accountability is stressed, requiring a detailed audit trail and logging. See Susan Biagi, *How the Government Looks at Security*, STACKS: THE NETWORK J., Dec. 1994, at 37.

The NSA has responsibility for classified national security issues, while the National Institute of Standards & Technology is responsible for non-classified information. Their guidelines are two of only a few published standards on computer system security, and commercial-sector standards are derived therefrom. *Id.*

56. Bob Melford, "Six-0" For Security and Things That Take Six Years, DIGITAL NEWS & REV., Sept. 27, 1993, at 11.

57. Cf. Roger Addelson, *Making Your Customer's Network Secure*, STACKS: THE NETWORK J., Dec. 1994, at 27. For an explanation of what constitutes C2 compliance, see *supra* note 55.

NetWare 4.x, Windows NT Server, Trusted Network Computing Environment and Cordant's Assure are C2 certified.⁵⁸

Individual work station security is also related to LAN security because workstations can be used as unauthorized ports of entry. Disk, screen and keyboard locking mechanisms can be used to prevent unauthorized access when employees are away from their computers. In addition, certain programs prevent unauthorized alteration of configuration and startup files (e.g. CONFIG.SYS and AUTOEXEC.BAT) and/or notify SysAdmins of any attempts to change program initiation (i.e., authorization specification) files. Finally, armoring products either prevent computer-booting through the floppy drive where password security could be bypassed or prevent resetting of computer clocks to make former passwords or SuperUser access retroactive.⁵⁹ Fischer International Systems Corp. makes a suite of products which performs these and other protective functions.⁶⁰

Client computers and LANs which have modems are also vulnerable to external intrusion from outside the local network. A common, and effective, method of preventing this type of unauthorized entry employs a "call-back" protocol. An authorized user who wishes to dial in and use an office computer dials up the computer via its modem. The computer is programmed to allow remote use from only certain, pre-authorized phone numbers. Upon receiving the call-in, the computer terminates the connection, checks the number dialed from against its list of authorized numbers, and calls the user's computer back if the number is an authorized one. When the connection is reestablished, the user must log in and successfully complete the rest of the user identification and authentication challenges in order to initiate the remote session with the computer.

5. FIREWALLS

The Pentagon has 650,000 terminals and work stations; the military has 10,000 local computer networks and 100 long-distance computer networks. The Pentagon currently experiences an average of two hacker attacks per day, "more than double the rate of 255 a year in 1994."⁶¹ Intruders have stolen, altered and even erased Pentagon

58. *Id.*

59. See Horace Labadie, *Digital Crime Watch: Developing an Effective Security System*, COMPUTER SHOPPER, Mar. 1994, at 594.

60. *Id.*

61. John J. Fialka, *Pentagon Studies Art of 'Information Warfare' To Reduce Its Systems' Vulnerability to Hackers*, WALL ST. J., July 3, 1995, at A20.

records.⁶² Robert Ayers, chief of the Defense Information Systems Agency's (DISA) information warfare division, acknowledges that the Pentagon's electronic infrastructure is "not safe and secure."⁶³

The Department of Defense (DOD) developed firewalls for computers and networks in the mid-1980s in order to prevent access to, and leaking of, classified documents.⁶⁴ Firewalls create a shell of protection between a network and possible intruders.⁶⁵ Although they are commonly used to restrict information from exiting or entering a firm's computer or LAN via a modem, firewalls are increasingly being designed and integrated into routers/gateways in order to regulate the flow of information between a LAN and the Internet.⁶⁶ The firewall typically sits on the router and functions by filtering all the electronic data packets sent to it from the LAN and the outside connection.⁶⁷ Only verified electronic data packets are passed on by the firewall's packet filter, assuming the firewall is properly configured. For example, a firewall may be configured to accept (and process) only e-mail type communications data-packets and to accept mail for only a particular set of addressees. In such a case, an intruder attempting to initiate a file-transfer request would be thwarted, as the firewall would not recognize the communications protocol and would thus reject it. In fact, without the proper server program on the host computer, the computer would have no way of responding to such a request.

Vendors offer a wide array of firewalls to provide protection to Internet routers/gateways.⁶⁸ For example, Network Systems markets

62. Bernstein, *supra* note 12, at 49.

63. Munro, *supra* note 23, at C3.

64. Gary H. Anthes, *Hackers Stay a Step Ahead*, COMPUTERWORLD, Oct. 17, 1994, at 14.

65. The purpose of a firewall is to protect sensitive information. Mass-marketed firewall software products include FireWall-1, sold by CheckPoint Software Technology Inc. of Lexington, Massachusetts. FireWall-1 is installed like any other mass-marketed, pre-packaged software without any customized modifications. See generally Streeter, *supra* note 4, at 58. Commercial entities will frequently design their own firewall using an Internet security consultant. Network managers will hire security consultants to design not only firewalls but also network security policies for firms. *Id.*

66. Firewalls for UNIX-based software gateways are increasingly being designed to perform packet filtering. Firewalls are usually part of a larger network security policy employing other protection such as password protection, data encryption and workstation security. *Id.*

67. Routers attached directly to the Internet will use "packet filters." "Packet filters are essentially rule-based programs that instruct a router to accept only certain types of traffic from specified network addresses." Ted Doty, *The Whole Truth About Network Security*, DATA COMM., Nov. 1994, at 150.

68. Some users also employ public-domain firewall tools such as SOCKS. Streeter, *supra* note 4, at 58.

BorderGuard for the protection of remote sites. Another product employs proxies, which are "slimmed-down versions of applications that are open to outside users and serve to protect the 'real' application behind the firewall from bugs."⁶⁹ IBM's "NetSP Gateway" enforces network access rights based on user-determined rules. It also takes action if hacking is suspected based upon an analysis of address pairs and requested services.⁷⁰ Harris Corp. makes a computer safeguard called CyberGuard Firewall, which places a computer between a company's LAN and its outside connections.⁷¹ Trusted Information Systems, Inc. developed Gauntlet, a firewall based on Pentium hardware, using a modified version of Unix.⁷² Firewall technology has evolved considerably in recent years and now provides significant protection against the unwanted inflow or outflow of digital data.

6. PASSWORDS

Passwords were one of the earliest security "devices" developed in the mainframe environment to keep out intruders. Passwords have been less than successful in thwarting security breaches in the LAN environment because of cultural attitudes toward their use and dissemination. A commentator illustrated the lackadaisical attitude toward passwords in a recent demonstration at a conference. Posing as a computer room operator, the security expert simply called the switchboard operator of the local telephone company. The operator willingly provided the impostor with a "critical, top-secret password" granting access to a database of the names and addresses of all of its customers, the "crown jewels" of the telephone company.⁷³ In these cases, the breach does not occur across the Internet, but rather through socially-engineered dial-in access. This type of low-tech hacking is an area where telephone hackers, known as "phrEakers" or "phrackers," have been able to wreak havoc with company computers and telephone accounts.

Other breaches occur via the Internet due to careless password security. The British hacker Paul Bedworth was able to enter

⁶⁹. Joanie Wexler, *Users Send Out an SOS to Internet Providers*, NETWORK WORLD, Feb. 13, 1995, at 37.

⁷⁰. *See id.*

⁷¹. Frank Ruiz, *ECI to Build E-Mail Security Chip for U.S.*, TAMPA TRIBUNE, June 8, 1995, at Business and Finance 1.

⁷². Knowles, *supra* note 30, at 14.

⁷³. Susan Watts, *The BT Hacker Scandal: BT 'Flouted its Own Advice to Government,' Consultants Are Fighting a Losing Battle to Persuade Firms to Protect Their Computer Systems*, THE INDEPENDENT, Nov. 25, 1994, at 3.

numerous government and company computers because they were protected only by the password of the installing engineer or another simple default.⁷⁴ It is estimated that "over half of the passwords in use are said to be the first names of spouses and children, birthday and anniversary dates, and the names of super-heroes."⁷⁵ Passwords such as these are highly susceptible to security breach because a hacker (either a company insider or a remote hacker using the Internet or dial-in access) need only run a hacker dictionary program against the target computer in order to learn the password and thereby access the computer itself.

Hacker dictionary programs operate by trying every word in the dictionary (including variants of words and names) until a password match is found. The shorter the password, the faster it will be cracked. Given the comprehensiveness of these dictionary programs and high speed of computers, common passwords can be broken within minutes or hours. If the vulnerable password is on a router/gateway computer, then the company is making its system vulnerable not only to insiders, but to Internet hackers as well. Fortunately, even a minimalist security program can detect such attempts and set off an alarm. In addition, increasingly effective password-protection schemes are available for implementation. These methods include: "pass-phrases," as opposed to mere pass-words; two-factor identification, which requires inserting a card or "token" belonging to the user along with inputting the proper password; dynamic synchronized password schemes which change the password in both the host and the user token every few seconds; and software-token-based challenge-response systems which use encryption to ensure all transactions are secure.⁷⁶ An example of an advanced password product is one which combines two-factor identification with dynamic synchronization. The password on the synchronized card changes every thirty to sixty seconds, and thus is good only for the duration of a single log-on session.⁷⁷ More secure—and expensive—methods of authenticating user identity are also proliferating.⁷⁸ These advanced methods include verification by retinal scanning,

74. *Id.*

75. Eric H. Steele, *Software Review: Security*, 5 COMPUTER COUNSEL 39 (Aug. 1993).

76. For a description of these and other password security schemes, see Winn Schwartau, *New Keys to Network Security*, INFO WORLD, May 15, 1995, at 51.

77. This smartcard is called SecurId and is manufactured by Security Dynamics, Inc., of Cambridge, Massachusetts. Another smartcard vendor is Enigma Logic, Inc., which produces a product called Safeword. Tom McCusker, *Take Control of Remote Access*, *Network Security Measures*, DATAMATION, Apr. 1, 1994, at 62.

78. Encryption may be used to protect passwords and data, and to verify communications.

fingerprint identification, signature recognition, voice recognition and biometric recognition, which is based on the unique way each user has of inputting her password or pass-phrase.⁷⁹

Even a computer defended with state-of-the-art security will not remain impregnable for long if no on-going efforts are directed toward security. High-tech hackers continually attempt to find new means of obtaining unauthorized access to computer systems. Like automobile anti-theft devices, computer, network and Internet security devices become vulnerable to breach over time. Steps must be taken continually to stay ahead of malefactors' resourcefulness. One recent hacker innovation, known as "spoofing," has proven successful against systems. This technique attempts to access otherwise secure systems by breaking the code words on one computer in a network, then impersonating the "friendly" machine to bypass the defenses of others.⁸⁰ To avoid this risk, SysAdmins should implement programs which adopt a norm of mutual suspicion and demand more thorough authentication.

7. ENCRYPTION

Encryption refers to any algorithm applied to a digital message which scrambles the plain text message, rendering it meaningless to anyone who does not have the key to decrypt the message. The federal government has used Data Encryption Standard (DES),⁸¹ a 56-bit, single key encryption technology, since the mid-1970s for its sensitive, but not classified, information.⁸²

One network security firm makes use of the International Data Encryption Algorithm, the DES and DES III algorithms.⁸³ The firm employ(s) a complex set of software services to connect a secured, corporate network to an unsecured network, such as the Internet. They can be configured to control access, authenticate users, hide some or all of a corporate network to the public and protect live corporate data by permitting access to only parts of applications.⁸⁴

79. Schwartau, *supra* note 76, at 51.

80. See generally RUSSELL L. BRAND, *COPING WITH THE THREAT OF COMPUTER SECURITY INCIDENTS: A PRIMER FROM PREVENTION THROUGH RECOVERY* (1990) (provides simple and cost-effective methods for preventing computer security problems and for incident handling and recovery. Available in USENET newsgroup comp.security.misc).

81. *The Data Encryption Standard*, in FEDERAL INFORMATION PROCESSING STANDARD 73 (1970).

82. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 736 (1995).

83. Roberts, *Network Systems*, *supra* note 30, at 1.

84. Wexler, *supra* note 69, at 37.

Encryption technology is expected to significantly advance the security of on-line commerce. However, encryption technology will not remain secure if the technology becomes outdated or compromised. For instance, the National Institute of Standards & Technology (NIST), while re-authorizing the government's use of DES in 1993, simultaneously indicated the approaching end of its usefulness.⁸⁵ Due to the yearly near-doubling of computer speed and power, breaking an encryption key through "brute force" takes less and less time.

Until recently, all of the most secure systems used single key algorithms.⁸⁶ The new public key/private key encryption technology, such as that incorporated into RSA⁸⁷ encryption technology, is being hailed as a practical solution for secure Internet transactions.⁸⁸ RSA is marketed by RSA Data Security of Redwood City, California, and it has become the de facto encryption industry standard.⁸⁹ It is built into current or planned O/Ss for Microsoft, Apple, Sun and Novell.⁹⁰ It is also used in secure telephones, Ethernet network cards and smart cards.⁹¹

RSA's public key/private key encryption technology⁹² has two advantages over previous encryption technologies.⁹³ First, the addition of the private key, which is known only to the sender, adds an additional layer of security. With DES, each party had to simultaneously know the secret key. With RSA, the public key is published widely but the private key is held by only one person. Assuming the private key is not disclosed, the result is message confidentiality and transmission security. Thus, when the sender

85. Froomkin, *supra* note 82, at 738 n.120.

86. See BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 273-74 (1994). See generally *id.* at 219-320 (providing extensive information on block cipher encryption schemes such as DES and public key encryption schemes such as RSA).

87. "RSA" stands for the names of its MIT inventors: Ron Rivest, Adi Shamir and Leonard Adleman. The RSA algorithm was introduced in 1978. SCHNEIER, *supra* note 86, at 281-82.

88. Liu, *supra* note 2.

89. See RSA'S FREQUENTLY ASKED QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY 8 available on RSA's Web site: "http://www.rsa.com/rsllabs/faq/faq_rsa.html#rsa.1" (hereinafter RSAFAQ).

90. *Id.*

91. *Id.*

92. Public key cryptography was invented in 1975 when Whitfield Diffie published an article conceptualizing it with the assistance of Martin Hellman, a Stanford University computer scientist. RSA algorithms can also be found in Phil Zimmerman's Internet-distributed program entitled "Pretty Good Privacy" (PGP). Public key cryptography is likely to be popular in the Privacy Enhanced Mail program (PEM), as well.

93. See generally EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 30 (1994) (explaining public key encryption).

("A") transmits a message using the recipient's ("B") *public key*, only the proper recipient, B, has the *private key* necessary to decode it. Conversely, when sender A transmits a message encoded with her own *private key*, any recipient with sender A's *public key* can decode it, but the *private key* acts as a digital signature, authenticating that A is in fact the sender and that the message has not been altered. Barring what is known as a "man in the middle" security breach, recipient B knows the message could only have been sent by A.

While public key processing has the disadvantage of being about 100-times slower in software and 1,000 times slower in hardware than DES,⁹⁴ various methods are already circulating to mitigate this shortcoming. One solution is to use RSA primarily to transmit brief messages. For longer messages, RSA encryption can be used to send the recipient a one-time single key encryption scheme, which then can be used to send the subsequent long message.⁹⁵ Since the single key encryption scheme is used only one time, the security of the transmission is not compromised. A third method, known as "RSA digital envelope," combines DES and RSA as follows: "[F]irst the message is encrypted with a random DES key, and then, before being sent over an insecure communications channel, the DES key is encrypted with RSA. Together, the DES-encrypted message and the RSA-encrypted message are sent."⁹⁶

RSA's second major advantage is that its keys are functions of a pair of extremely long prime numbers for which no factoring algorithm is currently known.⁹⁷ If hackers could discover a factoring algorithm or other cryptanalysis scheme for RSA, they would have a "shortcut" to breaking RSA keys.⁹⁸ Until and unless a factoring algorithm is discovered, however, hackers are reduced to trying to break keys by "brute force." This entails systematically trying every combination of numbers, letters, or symbols which conceivably could comprise the key until the proper combination is found.

Michael Froomkin describes the mammoth resources needed to crack a 129-digit RSA key by brute force:

A group of computer scientists and mathematicians recently used the Internet to harness computer time donated by 600 volunteers. Using a total of about 5,000 MIPS-years [approximately the equivalent of the power of 33 100 Mhz Pentiums running for a year] of processing time to make 100

94. SCHNEIER, *supra* note 86, at 285.

95. *Id.*

96. RSAFAQ, *supra* note 89.

97. SCHNEIER, *supra* note 86, at 282.

98. *Id.* at 284.

quadrillion calculations over an eight month period, the group solved a problem equal in complexity to breaking a 129-digit RSA key.⁹⁹

Michael Froomkin notes that the increasing potential of parallel processing "might make it possible to break even a 512-bit [64-digit] key at a cost . . . well within the means of the poorest government."¹⁰⁰ While this may be so, common sense dictates that any foreign governments attempting to crack RSA keys will direct their efforts at high-level federal offices or corporate institutions. In addition, while governments may have the resources to crack a 64-digit RSA key, most RSA keys are two to three times longer than that. The longer the key, the greater the security. Entities with very high security needs can use long keys and combine them with additional measures to assure security. The average American's on-line commerce should suffer no risk from foreign intrusion because the cost so outweighs the gain as to make it impractical.

With regard to private hackers, it is doubtful that even the most determined ones will be able to marshal the necessary resources to crack 64-digit RSA keys. While a student at France's Ecole Polytechnique in Paris cracked an RSA-based key on Netscape's browser in August of 1995 by running a network of 120 computers for eight days,¹⁰¹ the keys were only five digits or less in length.¹⁰² In addition, the "serious security flaw" discovered in Netscape's domestic browser in September of 1995 by two computer science students at the University of California at Berkeley was due to Netscape's flawed random-number generating system, not the RSA key itself.¹⁰³ The company announced it would incorporate a more complex coding formula plus a coding string ten times longer than its predecessor.¹⁰⁴ One industry expert markets encryption systems using 170-digit RSA keys and flatly asserts they are "unbreakable."¹⁰⁵

99. Froomkin, *supra* note 82, at 740.

100. *Id.* at 888. Professor Froomkin cites an estimate that a 512-bit [64 digit] key can be broken with approximately \$8.2 million worth of equipment. *Id.* at 775.

101. John Markoff, *Software Security Flaw Put Shoppers on Internet at Risk*, N.Y. TIMES, Sept. 19, 1995, at A1.

102. It takes eight "bits" of information to create a single digit, or character, in computer language. Although the Clinton Administration is considering allowing the export of encryption code of up 64 bits, the maximum-length encryption code currently exportable is 40-bit. Forty bits of information would produce a maximum of five digits or characters. *New Policy Proposed on Software Protection*, ATLANTA J. & CONST., Aug. 20, 1995, at 6.

103. Markoff, *supra* note 101, at A1.

104. The coding string will be essentially a 50-digit RSA key. *Id.*

105. Daniel M. Federman, President, Premenos, *Protecting Enterprise Information in the Digital Age: Encryption, Digital Telephony, Privacy and Security*, Presentation

Given the growing recognition of the security assurance provided by public key cryptography, major corporations and institutions are forging ahead with schemes for on-line commerce. The latest version of Netscape's World Wide Web browser supports RSA encryption, which is designed to facilitate secure Internet transactions. MasterCard has been working with Netscape Communications Corp. to effectuate secure electronic commerce.¹⁰⁶ Visa International, Inc. has undertaken a joint venture with Microsoft Corp. to develop a software program that will allow customers to make secure credit card payments over the Internet by making use of passwords.¹⁰⁷ Europay, Europe's largest credit card company, initiated a joint venture with International Business Machines Corp. in June to develop a scheme for conducting secure business over the Internet.¹⁰⁸

8. DIGITAL SIGNATURES

"Digital signatures," designed to insure against falsification or alteration,¹⁰⁹ are also becoming part of the accepted legal infrastructure in the information security field. This technology, which employs cryptography to secure information, also provides a

at the American Bar Association Section of Science & Technology Annual Meeting (Aug. 7, 1995).

106. *Visa, MasterCard Plan Internet Venture*, L.A. TIMES, June 23, 1995, at D3.

107. *Id.*

108. *Id.*

109. The ABA Science and Technology Section guidelines describe digital signatures as being

created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. For digital signatures, two different keys are generally used: one for creating a digital signature or transforming data into seemingly unintelligible form, a process often termed "encryption," and another key for verifying a digital signature or returning the message to its original form, a process often termed "decryption."

Computer equipment and software utilizing two such keys is often termed an "asymmetric cryptosystem." The keys of an asymmetric cryptosystem for digital signatures are termed the *private key*, which is known only to the signer and used to create the digital signature, and the *public key*, which is ordinarily more widely known and is used to verify the digital signature. A recipient must have the corresponding public key in order to verify that a digital signature is the signer's. If many people need to verify the signer's digital signatures, the public key must either be distributed to all of them or published in an on-line repository or directory where they can easily obtain it.

Information Security Committee, American Bar Association, DIGITAL SIGNATURE GUIDELINES WITH MODEL LEGISLATION 22 (Provisional Draft, July 26, 1995).

means of identifying the sender.¹¹⁰ The goals of an effective digital signature system are to achieve signer authentication, document authentication, affirmative acts signifying a signature and efficiency.¹¹¹ The ABA "Digital Signature Guidelines" seek to: 1) minimize the incidence of electronic forgeries; 2) enable and foster the reliable authentication of documents in computer form; 3) facilitate commerce by means of computerized communication; and 4) give legal effect to the general import of the technical standards for authentication of computerized messages.¹¹² Digital signatures, like encryption technology in general, secure electronic transactions from point of origin to point of receipt.

9. THE ODYSSEY OF THE GOVERNMENT'S CLIPPER CHIP

The National Security Agency (NSA) designed the so-called "Clipper Chip," with the single-key based algorithm SKIPJACK, to defeat cellular-based security breaches.¹¹³ Its purpose was to prevent private parties from using encrypted cellular-based communications for illegal purposes.¹¹⁴ The original plan for the Clipper Chip entailed a tradeoff: the government would provide the private sector with encryption technology certified by the NSA as unbreakable for years to come, and recipients would allow government agencies to hold their secret keys in escrow.¹¹⁵ The keys would be divided into two parts and housed with escrow agents at two different government agencies, the Treasury Department's Automated Systems Division and the Commerce Department's NIST, both executive-branch offices.¹¹⁶ The escrowed keys could only be obtained for a given purpose by law enforcement officers exercising legal warrants.¹¹⁷ The secret keys would allow law enforcement to decode Clipper-encrypted

110. *Id.* at 31.

111. *Id.* at 20-21.

112. *Id.* at 33.

113. *Privacy Issues in the Telecommunications Industry: Testimony Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 103d Cong., 2d Sess. (1994) (statement of Stephen T. Walker, President, Trusted Information Systems).

114. See Stephanie Stahl (with Mary E. Thyfault), *About Face on Clipper—Privacy Advocates Draw Conflicting Conclusions on Encryption Policy*, INFO. WK., Aug. 8, 1994, at 24.

115. Froomkin, *supra* note 82, at 715-16.

116. See Rochelle Garner, *Clipper's Hidden Agenda*, OPEN COMPUTING, Aug. 1994, at 54.

117. *Id.* at 54

communications. A similar system was envisioned with regard to data-based information utilizing the Capstone algorithm.¹¹⁸

Clipper and Capstone have stirred considerable controversy. They are opposed by civil libertarians who view the government's ability to break strong cryptography at will as the predecessor of Big Brother.¹¹⁹ Others oppose them on constitutional bases.¹²⁰ Those with commercial interests fear that a product the U.S. government can tap into "at will" will be anti-competitive on foreign markets, as well as at home.¹²¹ Global marketeers maintain that the true agenda of Clipper/Capstone is to ensure that the NSA retains control over exports.¹²²

On the other hand, at least one nationally respected security analyst argues that not only law enforcement officials, but also regulatory agencies such as the Securities and Exchange Commission, the Food and Drug Administration and the Atomic Energy Commission should have access to the keys: "All [such agencies] must have the capability to eavesdrop on the industries they watch over under hostile circumstances. Because if we have powerful cryptography freely available to our citizens, and the government does not have an eavesdropping capability, our democracy will be destroyed."¹²³

Given the controversy and opposition, it is unlikely that Clipper and Capstone will succeed in their original form. A representative of the Federal Bureau of Investigation reports that progress is being made with the Clipper initiative.¹²⁴ The federal government has agreed to allow Clipper keys to be escrowed with private entities rather than governmental agencies. Foreign governments are more receptive to the idea since they share with the U.S. the objective of deterring terrorists.¹²⁵

118. Allan McDonald, Federal Bureau of Investigation, Protecting Enterprise Information in the Digital Age: Digital Telephony, Privacy and Security, Presentation at the American Bar Association Section of Science & Technology Annual Meeting (Aug. 7, 1995); see also Froomkin, *supra* note 82, at 715-16 n.16.

119. See Garner, *supra* note 116, at 51 (describing the Clipper Chip controversy).

120. See Froomkin, *supra* note 82, at 810 (discussing personal privacy, freedom of association, free speech, unreasonable search and seizure, and potential self-incrimination issues in the context of a governmental mandatory encryption key escrow scheme, which some commentators believe to be implicit in the Clipper initiative).

121. Garner, *supra* note 116, at 52.

122. *Id.*

123. *Id.* at 52 (quoting Donn Parker, program manager of information and security, SRI International, Menlo Park, Cal.).

124. McDonald, *supra* note 118.

125. *Id.*

Meanwhile, the government has legitimated public/private key encryption technology. This is apparent in the recent establishment by the U.S. General Services Administration (GSA) and the DOD of an office whose task is to implement the "highest standards" of security within the government's electronic system by implementing a "public key encryption infrastructure and the widespread capability to handle secure digital signatures."¹²⁶

10. AUTHENTICATION OF ELECTRONIC COMMERCIAL TRANSACTIONS

The optimism that the security problem can be solved has led to recent exponential growth of electronic commerce.¹²⁷ For example, "ExpressNet," recently developed by the partnership of American Express and America Online, permits consumers to pay bills and download their billing histories along with a history of recent transactions directly into their computer's financial-management software.¹²⁸

Banking on the Internet will soon flourish in a secure environment thanks to joint ventures between MasterCard International and Netscape Communications Corp., and between Visa International and Microsoft.¹²⁹ Another firm has introduced a product which purportedly enables organizations to exchange information in total confidentiality across all types of private and public access data networks, including the Internet.¹³⁰

Consumers also may now access their credit cards from "electronic wallets" displayed on their computer screens and consummate financial transactions without having to set up special accounts with businesses in advance.¹³¹ Many companies are racing to introduce digital money, or "E-Cash" systems; Citicorp is developing an "entire infrastructure for using electronic money to be issued by Citicorp and

126. Kennedy Maize, *GSA & Department of Defense Open Information Security Offices*, NEWSBYTES, May 24, 1995, available in USENET Newsgroup clari.nb.govt., Article 707 (emphasis added).

127. See, e.g., *Technology Briefs*, THE PLAIN DEALER, Apr. 9, 1995, at 4l.

128. Jared Sandberg, *American Express Goes On-Line for Card Holders*, WALL ST. J., Jan. 30, 1995, at A3.

129. *Id.*

130. See, e.g., Micahel Csenger, *NSC Unveils Next-Generation Router/ATM Campus Switch*, NETWORK WORLD, Nov. 14, 1994, at 3; see also, *ATM: Network Systems Corp. Introduces Networks-On-Demand on New Enterprise Routing Switch: Single Platform Combines Routing & Switching With ATM Connectivity*, EDGE, Nov. 14, 1995.

131. *Technology Briefs*, *supra* note 127, at 4l.

other banks."¹³² Even an automated clearing house for mutual funds is slated for the Internet by Galt Technologies' "NETworth" service.¹³³

11. COMBATING THE ENEMY WITHIN ORGANIZATIONS

While encryption seems to be providing a solution to the problem of insecure Internet transactions, many firms are still failing to take adequate internal security measures to protect against computer security breaches by their employees. Ernst & Young's study of 1,271 companies concluded that slightly more than a third of firms perceived their senior management as being only slightly concerned with information security.¹³⁴ Eight percent indicated that their management perceived security issues to be not important at all.¹³⁵

One in four companies have sustained losses from network security breaches in the past two years, many of which were committed by disgruntled employees or ex-employees.¹³⁶ For example, a bank officer attempted to embezzle \$15.1 million by electronically transferring funds into his own Swiss account.¹³⁷ An ex-employee at another company was allegedly caught, three months after being fired, in the act of downloading proprietary software from the company's computer. A password she had shared with five other employees had not been changed after her dismissal. She was able to spend eighteen hours copying programs before a phone trace led to her arrest.¹³⁸

Detection of internal misappropriation is a much more complicated issue than locking the doors at night; however, effective deterrence is attainable through implementation of adequate security measures. It is recommended that, in the event of a hostile employee termination, an escort should accompany the ex-employee while he cleans out his office and transfers any security codes back to the firm.¹³⁹ Any security code that was in the hand of a disgruntled ex-employee should be presumed compromised. Passwords and other

132. Kelley Holland & Amy Cortese, *The Future of Money: E-Cash Could Transform the World's Financial Life*, BUS. WK., June 12, 1995, at 66.

133. *Cyberspace Comes to Mutual Funds in Next Wave of "Home Banking,"* BANK MUTUAL FUND REP., May 31, 1995, at 1.

134. Jared Sandberg, *Losses Linked to Lax Security of Computers*, WALL ST. J., Nov. 18, 1994, at B4.

135. Thirty-four percent of respondents believed that information security was viewed by their managers as only "somewhat important." *Id.*

136. Addelson, *supra* note 57, at 27.

137. *Id.*

138. *Id.*

139. *Protecting Your Data When Firing Employees: A Sensible Precaution*, ROCKY MOUNTAIN NEWS, Dec. 3, 1994, at A71.

security devices must be changed within a few hours. Surrendering of access codes should have the same status as returning keys, credit cards and building access credentials.¹⁴⁰ An essential part of changing access codes is keeping a good record of all access by the ex-employee.

In-house computer system security can be rendered meaningless if passwords are written down, known to others, shared, easily guessed, or subjected to hacker dictionary programs. The insider-practice of "shoulder-surfing" to steal the passwords of users who have broader access privileges represents a potentially greater threat to computer system security than outside hackers.¹⁴¹ Current password protocols are acknowledged to be "often inadequate to prevent unauthorized access to a computer system."¹⁴² The current overwhelming ignorance and indifference toward password security in companies constitutes one of the greatest threats to computer systems' security. Yet it is a self-inflicted wound. The patient can cure himself quite easily with a little effort and minimal resources. Informal password protocols are already available, and tailored formal versions can be implemented within companies with relative ease. Although password security and adequate employee-access security require implementing special security policies, their proper implementation should virtually eliminate the occurrence of computer break-ins by insiders.

B. The Internet/Network Security Industry

Prior to the mass-marketing of the Internet, computer system security was essentially lore developed and shared by SysAdmins who communicated electronically on newsgroups dedicated primarily to discussion of Unix-based systems. This dialogue about Unix security loopholes and remedies provided the basis for today's network security industry. With the PC revolution and advent of the National Information Infrastructure, companies and organizations began to recognize the security risks inherent in their in-house computer systems. They called in these Unix "experts" to analyze risk and recommend and implement security solutions. The commercial network security industry was born.

Commercially, the industry is still young. There are no nationally-recognized standards for classifying persons as "network

140. Steele, *supra* note 75, at 35.

141. Michael P. Dierks, *Symposium: Electronic Communications and Legal Change: Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 311-12 (1993).

142. *Id.* at 311.

security consultants,"¹⁴³ and such consultants have not been deemed by courts to comprise a "profession."¹⁴⁴ Nevertheless, the emergent industry has rapidly progressed from providing pure consulting services to companies with Unix mainframes on an ad-hoc basis to developing a number of countermeasures to mitigate the danger of unauthorized access, theft, or damage to a computer's intangible electronic data. Like home break-ins, computer intrusion can be combated by a spectrum of methods and products. The various components and considerations discussed in the previous part can be applied singly or in combination to achieve the desired level of safety from Internet intrusions as well as in-house hackers. For example, company employees who encrypt sensitive e-mail communications are protecting the company against in-house security breaches as well as Internet hackers. In these cases, "network" security truly is synonymous with "Internet" security. Other countermeasures are designed more specifically to thwart either Internet or in-house security breaches.

The majority of network security solutions are like the intangible electronic data they are designed to protect in that they are computer programs. Since the 1980 amendment to the Copyright Act, software has been specifically recognized as copyrightable.¹⁴⁵ This protection has had a significant impact on the industry by introducing intellectual property considerations. Complicating the arrangement is the fact that software programs are not sold; they are licensed. This problem will be discussed in part IV. Not all security solutions, however, are software. Many are combination software/hardware solutions. Some are pure intangibles, and others pure personnel policy. Some consist of security consultant services leading to personnel or SysAdmin protocol recommendations. The major categories of

143. Major players in the computer industry support their own certification programs, which can provide some guidance in assessing a proclaimed network security professional's competence. For example, Microsoft provides a certificate to those individuals who pass Microsoft's exam on Windows NT. Windows NT is Microsoft's renowned operating system for networks which are C2 compliant. A customer shopping for a network security professional would thus have fair assurance that such a certified individual would have the expertise to install, configure and maintain a Windows NT server and network in a secure operating manner. See BECOMING A MICROSOFT CERTIFIED PROFESSIONAL, available at "http://www.microsoft.com/moli/advising_building/certifications/introduction-to-certification.html" on the World Wide Web.

144. See *infra* note 176 and accompanying text.

145. H.R. REP. NO. 1307, 96th Cong., 2d Sess. 23 (1980), reprinted in 1980 U.S.C.A.N. 6460, 6482; 17 U.S.C. § 101 (definitions), 109 (limitation on exclusive rights of copyright owner), 117 (special provision providing for noninfringement of certain uses of computer programs).

commercial security solutions that have developed to date are outlined below.

1. MASS-MARKETED NETWORK / INTERNET SECURITY PRODUCTS

Most security products are software, sets of instructions housed on diskette or CD-ROM that are designed to perform designated security functions. The simplest examples are programs which perform a single primary security function, such as anti-virus programs. Prime examples are Norton Anti-Virus and McAfee Anti-Virus. More sophisticated programs offering more comprehensive protection are also available as mass-marketed software products. For example, Norton's Disklock can be used on a single computer or a network to restrict access to hard drives, directories and files to authorized users only. Like dead bolts and window bars for the home, software security products can be purchased and installed by the consumer to deter specific threats.

2. OWNER-DISTRIBUTED SECURITY PRODUCTS

A significant portion of network security products are not mass-marketed, but are distributed by the developers themselves and/or their authorized representatives. Security products within this category include firewalls, as well as hardware and software access control products, such as Security Dynamics Technologies, Inc.'s Ace/Server and ACM, respectively,¹⁴⁶ and properly configured network servers, such as Cylink Corp.'s SecureManager.¹⁴⁷ Owner-distributed products are typically more complex than mass-marketed products. They are frequently a combination of hardware and software, and require more detailed installation and administration procedures. Despite their complexity, the trend in the industry is to market these products without a "services" component. Thus, the burden is on the customer to install and maintain the hardware and software correctly. The contract in Appendix A, "Example of a Sales and License Agreement of a Network Security Product," typifies this arrangement.

146. *Security Dynamics Expands Internet User Authentication Security*, BUS. WIRE, Sept. 26, 1995. Security Dynamics Technologies, Inc. of Cambridge, Massachusetts has gone even further and linked its two-factor SecurID passcode and its ACE/Server software access control product with Trusted Information Systems' Gauntlet firewall to "deliver a unique combination of undefeatable security with ease-of-use" in protecting networks from unauthorized access via the Internet. *Id.*

147. *Network Security*, NETWORK MANAGEMENT SYSTEMS & STRATEGIES, Sept. 19, 1995.

3. CUSTOMIZED SECURITY

Innovation and proliferation of security products has decreased the likelihood of a "network security professional" being called on to custom-develop a security product or system. In most instances, a security consultant will analyze the vulnerabilities of a system and remedy them with a combination of already-available services, tools and protocols. This is primarily a services transaction, as opposed to a sale or license. For instance, a network security consultant might conduct a security audit of the company's network to discover an improper or inadequate configuration of the network's server computer. The security consultant would then correct the vulnerability by properly configuring the server. Depending on the company's security needs, she might additionally recommend and install various security products, such as a program that requires users to change their passwords every thirty days or a digital notary system. Just as importantly, the consultant might advise the company on the adoption of personnel policies for protection against in-house and Internet hackers.

4. FREWARE AND SHAREWARE SECURITY TECHNOLOGIES

A number of Internet security technologies are pure intangibles. They are neither mass-marketed nor distributed by licensed dealers—they are simply available for downloading from the Internet. For example, a non-commercial version of the PGP encryption scheme was placed on the Internet for free dissemination by its creator, Phil Zimmerman.¹⁴⁸ This is an example of "freeware," software which can be downloaded from the Internet and used indefinitely without incurring any costs.

Security technologies also include "shareware." Like freeware, shareware can be downloaded directly from the Internet. Unlike freeware, it is provided on a trial basis for a limited time only, usually thirty days. Shareware operates on the honor system, allowing a user to "sample" the technology at no charge. If the user then decides to continue using it, she is expected to pay for and register the "product." Technically, nothing prevents a user from continuing to use technology that she has not paid for. However, disseminators of shareware can and do incorporate various payment incentives. For example, shareware technology is often scaled-down in capability from its registered counterpart. Registration entitles a

148. For a description of PGP, see *supra* note 92. For an excellent introduction to PGP and its use, see BACARD, *supra* note 44, at 125.

user to receive the full version, plus free updates and technical support. An example of a shareware security technology is McAfee's Anti-Virus program, which can be downloaded from McAfee's Internet site.¹⁴⁹

Freeware and shareware security technologies can be downloaded and used without the help of an Internet security consultant. Likewise, mass-marketed products that require little more than simple installation and provide menu-driven prompts for proper use do not require an Internet security consultant. Yet, these technologies and products form an important part of the Internet security industry. They are indicative of the manner in which Internet security is being made more readily available, more user-friendly and more seamlessly woven into every aspect of everyday computing. At this stage, network security consultants are still crucial for helping companies connected to the Internet protect their informational treasure troves. To do this, network security professionals employ an ever-increasing and effective complement of Internet security products, tools and protocols.

The basic building blocks of a secure Internet are already in existence and in use. Hardware and operating systems can be rendered reasonably secure when properly maintained and configured by trusted personnel. Network security products, such as self-diagnostic tools and firewalls, are critical to achieving this goal. Other security technologies such as encryption and digital signatures have demonstrated the ability to secure Internet transactions. Vulnerabilities such as weak passwords and unauthorized access can be remedied through several means. These include implementation of appropriate personnel policies, institution of more sophisticated password schemes or products, and installation and use of hacker detection programs. With today's availability of network security products and the use of proper security protocols, Internet security¹⁵⁰ is no longer the unreasonable proposition or "oxymoron" it was in the past.

III. THE QUESTION OF LEGAL STANDARDS FOR INTERNET SECURITY

This part examines liability for Internet security products in light of traditional tort and contract doctrine. As demonstrated in

149. McAfee's address on the World Wide Web is "<http://www.mcafee.com>."

150. Having explained the relationship between network and Internet security, this article hereinafter uses the term "Internet security" to encompass both network and Internet security.

part II of this article, Internet security products are vital to the successful development of the National Information Infrastructure. They are part and parcel of bringing American commerce and business on line. Yet, at present, the law is unclear as to how liability would be allocated in the event of an Internet security breach that results from a security product's failure. The law of computer bulletin boards has been called "a land with no maps and few native guides."¹⁵¹ The same is true of Internet security. This part analyzes results that could be obtained from applying negligence and strict products liability theories, as well as traditional contract theory and Article 2 of the Uniform Commercial Code (U.C.C.), to claims of Internet security breach. We find that each of these traditional doctrines and theories is ill-equipped to deal with the novel issues associated with the emerging security-related technologies.

A. Regulation Under Tort Law

Each episode of the 1940s radio program "The Shadow" commenced with a mysterious voice asking, "Who knows what evil lurks in the minds of men? . . . The Shadow knows."¹⁵² A sinister laugh followed. That laugh is emblematic of the seamier side of the Internet. The anonymity of Cyberspace grants its citizens the freedom to adopt virtual roles and status with impunity. There are no easy methods of punishing and deterring electronic stalkers, converters, defamers and other intentional wrongdoers. The entire purpose of the Internet security field is to offer products and services to counter the dangers of what Anne Branscomb calls "true anonymity in the Network."¹⁵³ Yet it is not clear who should bear the burden of security breaches.

Are Internet security and service providers liable under tort law for security breaches by anonymous Internet wrongdoers? The *Restatement (Second) of Torts* takes the view that any invasion of a legally protected interest, whether based in negligence, strict liability or intentional misconduct, can be punished under tort law.¹⁵⁴

151. Loftus E. Becker, Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted By Others*, 22 CONN. L. REV. 203, 205 (1989).

152. JOHN M. CARROLL, *CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE* xi (2d ed. 1991) (comparing the loss of privacy due to the government's assembling of data files with the loss of privacy inherent in the concept of an all-knowing Shadow).

153. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1641 (1995) (arguing that anonymity and accountability are conflicting values in Cyberspace).

154. RESTATEMENT (SECOND) OF TORTS § 6 (1965).

The following discussion applies negligence and strict products liability theories to the role of Internet security providers and identifies possible defenses available to them under tort law.

1. LIABILITY FOR NEGLIGENCE

One can be liable for negligence if one's conduct falls below the standard established by law for protecting others against unreasonable risk of harm.¹⁵⁵ In other words, negligence "is a departure from the conduct expected of a reasonably prudent man under like circumstances."¹⁵⁶ In the business context, this principle provides that a company, holding itself out as capable in its business, impliedly represents that it will perform its work with the "diligence ordinarily possessed by well-informed members of the trade or profession."¹⁵⁷

Before tort law can be applied to a new type of conduct, the appropriate standard of care must be established. Common law negligence does not define a level of care for Internet security providers, and ambiguities result when the historical means of establishing such a standard are employed. Moreover, no statute has been enacted to define Internet security standards. The application of negligence doctrine to the business of providing on-line services highlights these open questions and exemplifies why current negligence theory is ill-equipped to deal with Internet security liability.

a. Common Law Negligence

Many questions arise in trying to apply negligence theory to an Internet security breach caused by a failed security device. For instance, would the failure of an Internet security product be held to be like the barrel of flour that fell out of the miller's window and struck the passerby in the classic case of *Byrne v. Boadle*?¹⁵⁸ In *Boadle*, no evidence indicated that the miller was in any way negligent. The

155. *Pence v. Ketchum*, 326 So. 2d 831, 835 (La. 1976).

156. *Id.*

157. *Data Processing Servs., Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314, 319 (Ind. Ct. App. 1986); *see also* *Young v. McKelvey*, 333 S.E.2d 566 (S.C. 1985) (employee expressly or impliedly promising to perform work in a diligent and reasonably skillful manner); *Crank v. Firestone Tire & Rubber Co.*, 692 S.W.2d 397, 400 (Mo. Ct. App. 1985) (company claiming ability to perform work impliedly warrants that the work will be accomplished in a workmanlike manner); *Standard Roofing Co., Inc. v. Ragusa Bros., Inc.*, 338 So. 2d 119, 123 (La. Ct. App. 1976) (roofing company impliedly promises in every contract that work will be performed in a good and workmanlike manner).

158. 2 H. & C. 722, 159 ENG. REP. 299 (1863).

court held that the accident alone was prima facie evidence of negligence. If a hacker bypasses supposedly "hacker-proof" security devices, should the Internet security professional likewise be presumed negligent,¹⁵⁹ or should the plaintiff have the burden of showing that the security provided was unreasonably lax?¹⁶⁰

In addition, should we prefer rules or standards in setting the level of care for Internet security professionals? In the negligence context, *rules* generally prescribe the conduct which a person must follow in particular situations. For instance, motorists in the early twentieth century were required to stop, look and listen at a railroad crossing or be barred from recovery for railroad crossing injuries attributable to the railroad's negligence.¹⁶¹ In contrast, *standards* require only due care in the circumstances. While bright-line rules have the advantage of offering certainty, they lack the flexibility and ability to accommodate social change offered by standards.

Service aspects of Internet security products would most likely be actionable under negligence. In accord with common law negligence theory, the test for the Internet security service provider's exercise of due care would be objective: what care would a reasonable professional exercise under like circumstances?¹⁶² Assuming a

159. For the doctrine of *res ipsa loquitur* to apply, it must be more probable than not that defendant's negligence was the cause of harm. In addition, the defendant must be in exclusive control of the instrument causing harm, and the harm must not have been caused by any voluntary action on the part of the plaintiff. See *Newing v. Cheatham*, 540 P.2d 33 (Cal. 1975). A defendant cannot be held liable on mere conjecture (a computer may crash as result of a virus planted by a third party, but such is only one possible explanation of the unexplained loss of data) or the mere possibility of negligence (plaintiff suffers unfavorable reaction following administration by doctor of anesthetic). Likewise, absent a showing that defendant was in exclusive control, liability will not be imputed. See *Larson v. St. Francis Hotel*, 188 P.2d 513 (Cal. App. 1948) (holding that, because defendant did not have exclusive control over hotel room, liability under *res ipsa loquitur* did not apply to injuries caused by chair falling out of a room in defendant's hotel). Or, if a passenger is injured in a collision of a trolley with a truck, *res ipsa loquitur* will not apply against either the motorman or the truck driver. See William Prosser, *Res Ipsa Loquitur in California*, 37 CAL. L. REV. 183, 184-89 (1949).

160. The answers to these questions cannot be resolved with certainty due to the unique nature of information technologies. However, it would appear that the doctrine of *res ipsa loquitur* would not apply because of the difficulty of proving exclusive control of the dangerous instrumentality (i.e., the Internet security device).

161. *Baltimore & Ohio R.R. Co. v. Goodman*, 275 U.S. 66 (1927); but see *Pokora v. Wabash Ry. Co.*, 292 U.S. 98 (1934) (promoting caution in framing standards that amount to rules of law and specifically limiting the *Baltimore* decision).

162. *Blythe v. Birmingham Water Works Co.*, 156 Eng. Rep. 1046, 1049 (Ex. Ch. 1956) (holding that a public utility was not liable for "a contingency against which no reasonable man can provide").

plaintiff¹⁶³ could show sufficient deviation from the standard of care and resultant damages, a court could find a defendant Internet security services provider liable for damages. However, what would be the measure of the "reasonable professional" in this new profession? There is no currently-defined standard of care for Internet security professionals. Absent this definition, it is unclear how courts would interpret the duty of the "reasonable Internet security professional."

A beginning point for setting the standard of care for Internet security professionals could be to examine what is customary in the Internet security industry.¹⁶⁴ Widely shared norms could be the basis of a negligence lawsuit against an Internet security service provider who deviates from such norms.¹⁶⁵ However, compliance with an industry custom may be considered only the floor, and not the ceiling, in the setting of the standard of care.¹⁶⁶ In the field of Internet security, firms that conform to the most secure practices and comply with the best available technology would clearly satisfy the standard of reasonable care. The difficult question, however, would be, "How good is good enough?" If it is not customary for most firms to do security audits, will a firm that failed to perform such an audit be deemed to have satisfied the standard of reasonable care?

In *The T.J. Hooper*,¹⁶⁷ two tugboats were lost in a storm. The boats might have avoided disaster if they had been equipped with radios to receive the weather reports transmitted twice a day. The defendants defended on the basis that it was not customary to install radios in the boats. Judge Learned Hand rejected the defense of custom as a negligence "safe harbor." He stated:

[I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests . . . Courts must in the end say what is

163. The plaintiff could be a disappointed recipient of such services or a third-party beneficiary. Whether a duty was owed to the third party would likely be determined by the test of reasonable foreseeability: i.e., would an injured third party be within the zone of danger foreseen by the security professional?

164. Usage of trade is always relevant in assessing breaches of warranty under Article 2 of the Uniform Commercial Code. U.C.C. § 1-205 (1990).

165. It has been suggested that the doctrine of *res ipsa loquitur* could be applied to computer vendors, programmers and others participating in the construction of software. See Vincent M. Brannigan & Ruth E. Dayhoff, *Liability for Personal Injuries Caused by Defective Medical Computer Programs*, 7 AM. J.L. & MED. 123, 143 (1981). However, there is no case law on this possible approach to proving computer software negligence.

166. See generally Clarence Morris, *Custom and Negligence*, 42 COLUM. L. REV. 1147 (1942).

167. 60 F.2d 737 (2d Cir. 1932).

required; there are precautions so imperative that even their universal disregard will not excuse their omission.¹⁶⁸

By analogy, Internet security firms that provide lax Internet security may be found to be negligent if a judge finds that there are readily available security protocols or technologies that may reduce excessive and preventable risks of hacker entry.¹⁶⁹ Comparable judgments may be rendered against the companies who practice lax security in their firms, as well. Compliance with industry norms is not necessarily reasonable. Justice Oliver Wendell Holmes stated that "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not."¹⁷⁰

Efficiency may serve as a starting point for establishing "what ought to be done." The goal should be to reduce Internet information theft and security breaches to the point where the damages caused by such breaches equal the burden of precaution.¹⁷¹ Generally, in the negligence context, the traditional risk-utility formula is used to determine whether the cost of a precaution is warranted, i.e., whether the cost is less than the probability of harm multiplied by the gravity of the resulting injuries. Firms should not have to take precautions to prevent reasonably unforeseeable security breaches.¹⁷² The problem of using the traditional risk-utility formula in calibrating negligence in Cyberspace lies in the lack of empirical data. One must first identify the costs of security breaches and then estimate their probability. There is little empirical data on the probability of harm, the severity of the harm and the burden of precaution for most Internet security breaches. Without valid data, it is difficult to determine the optimal way to allocate costs, and courts have little recourse in setting a reasonable standard of care for Internet security professionals.

168. *Id.* at 740.

169. Custom should be one factor, not the end result in the negligence formula. See RESTATEMENT (SECOND) OF TORTS § 295(A) (1965).

170. *Texas & Pacific R.R. Co. v. Behymer*, 189 U.S. 468, 470 (1903).

171. We are indebted to Guido Calabresi's insight that accidents are social problems that society should attempt to reduce in an optimum and efficient way. See generally GUIDO CALABRESI, *THE COST OF ACCIDENTS* (1961). A similar argument can be made about reducing preventable security breaches on the Internet, although these are arguably not accidents.

172. The Learned Hand risk-utility balancing test would excuse an Internet security provider from taking precautionary measures when the costs of such measures are greater than the potential loss. In such case, it is not negligent to fail to avoid the accident. If precautions are not cost-efficient, society is better off without precautions. See *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d. Cir. 1947).

Assuming that reliable data could be obtained, an optimal standard of care for Internet security would be one that increases societal welfare (and wealth) in the long run. It should not promote over- or under-investment in security precautions because both would be economically inefficient and could stunt the development of Internet security products, the growth of an Internet security profession and development of the NII.

It is possible that Internet security professionals will ultimately be subject to a higher professional standard of care such as that currently imposed upon doctors, lawyers and accountants. To date, however, courts have been slow to recognize the tort of "computer malpractice."¹⁷³ The New York Court of Appeals has stated the view taken by numerous courts:

A profession is not a business. It is distinguished by the requirements of extensive formal training and learning, admission to practice by a qualifying licensure, a code of ethics imposing standards qualitatively and extensively beyond those that prevail or are tolerated in the marketplace, a system for discipline of its members for violation of the code of ethics, a duty to subordinate financial reward to social responsibility, and, notably, an obligation on its members, even in non-professional matters, to conduct themselves as members of a learned, disciplined, and honorable occupation.¹⁷⁴

Unlike law or medicine, there is no licensing body or minimal education requirement for computer professionals.¹⁷⁵ When presented with a claim for "computer malpractice," courts have *en masse* declined to create a new tort for computer professionals.¹⁷⁶ While it seems clear that actions for professional negligence against computer-related "professionals" are foreclosed at this time, a nationalized training of Internet security professionals may arise as

173. Thomas G. Wolpert, *Product Liability and Software Implicated in Personal Injury*, 60 DEF. COUNS. J. 519, 521 (1993).

174. *Lincoln Rochester Trust Co. v. Freeman*, 311 N.E.2d 480, 483 (N.Y. 1974).

175. Wolpert, *supra* note 173, at 521.

176. See *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D. N.J. 1979) (rejecting new tort of "computer malpractice" for those who render computer sales and service), *aff'd*, 635 F.2d 1081 (3d Cir. 1980); *Hospital Computer Sys. v. Staten Island Hosp.*, 788 F. Supp. 1351, 1360-61 (D. N.J. 1992) (stating computer consultants do not meet the standard of "professionals" and thus can be held liable only for ordinary, not professional, negligence); *Analysts Int'l Corp. v. Recycled Paper Prods., Inc.*, No. 85-C8637, 1987 U.S. Dist. LEXIS 5611 at *16 (N.D. Ill. 1987) (stating Illinois does not recognize tort of computer malpractice for computer software systems designers, marketers and installers); *Invacare Corp. v. Sperry Corp.*, 612 F. Supp. 448, 453-54 (N.D. Ohio 1984) (refusing to recognize business negligence in computer-related setting as computer malpractice).

the NII matures, and therefore professional malpractice might follow.

Liability of Internet security providers may, nevertheless, be reviewed under the common law standard of negligence. As discussed, however, the indefinite nature of the common law standard of care offers little guidance to Internet security providers attempting to calculate their risk and plan their behavior. It gives perhaps even less guidance to courts faced with the challenge of reviewing those calculations in the aftermath of a security breach.

b. A Statutory Standard of Care

When a standard of care is set by a legislative enactment or regulation, courts will often find a defendant who violates it negligent per se.¹⁷⁷ In *Osborne v. McMasters*,¹⁷⁸ a court imposed negligence liability on a pharmacist for supplying plaintiff's decedent with unlabelled poison in violation of Minnesota's food and drug act. The *Osborne* court explained:

It is now well settled . . . that where a statute or municipal ordinance imposes upon any person a specific duty for the protection or benefit of others, if he neglects to perform that duty he is liable to those for whose protection or benefit it was imposed for any injuries of the character which the statute or ordinance was designed to prevent, and which were proximately produced by such neglect.¹⁷⁹

The *Restatement (Second) of Torts* follows this principle in validating statutory or administrative definitions of the proper standard of care.¹⁸⁰ In the interests of promoting the development of the National Information Infrastructure, the United States government could extend its internal standards for network and Internet security to the commercial sector. If the federal government were to develop commercial-sector standards for Internet security,¹⁸¹

177. In the negligence context, § 286 of the *Restatement (Second) of Torts* requires that a plaintiff prove that she is a member of the class of persons protected by the statute; that the statute protects against the particular interest invaded; and that she suffered the particular harm or hazard that was envisioned by the statute. See also *infra* note 190 and accompanying text.

178. 41 N.W. 543 (Minn. 1889).

179. *Id.*

180. RESTATEMENT (SECOND) OF TORTS § 286 (1965).

181. "Tort law is overwhelmingly common (state) law . . ." W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 3, at 19 (5th ed. 1984). Congress, however, has been increasingly receptive to proposals to federalize tort law. The GOP's Contract with America, which calls for common sense legal reform, inspired both the House and the Senate to pass comprehensive federal tort reform bills in 1995. The Senate passed the Product Liability Fairness Act of 1995 which will preempt state tort remedies for products liability. See S. 565, 104th Cong., 1st Sess.

then computer/software product manufacturers, computer/Internet security consultants and companies using networks and the Internet could all be found negligent per se for violating a statutory security standard.¹⁸²

The National Computer Security Center of the NSA administers the process for C2 certification of computer security.¹⁸³ Assuming that a federal certificate authority were widely adopted,¹⁸⁴ an Internet security firm that, for example, failed to obtain necessary "trusted certificate" authority for validating digital signatures might be found negligent per se for any loss resulting from such failure. Network-security device vendors might be required to market products under these or even higher standards. For example, they could be required to market "sniffless password" products or services which meet the standard of one-time passwords, i.e., passwords which cannot be reused because they are never transmitted across the Internet or via a modem in plain text.¹⁸⁵ The NSA adopted a "sniffless password" system in the 1980s on its Dockmaster Computer. Commercial enterprises could be required to emulate the NSA's example.

(1995). The Senate bill is aimed primarily at restricting punitive damages in products liability. In March of 1995, the House of Representatives passed the Common Sense Legal Standards Reform Act of 1995, which is a more comprehensive bill that restricts remedies in every substantive field of tort law. See H.R. 956, 104th Cong., 1st Sess. (1995). The nationalization of tort restrictions is presently stalled pending the reconciliation of differences between the Senate and House bills. See *House, Senate Set to Appoint Conferees on Product Liability Measure*, BNA WASHINGTON INSIDER, Oct. 30, 1995.

182. De facto evaluation of security products *vis-a-vis* government standards is already occurring. Novell, Inc. announced in August that they have formally applied for federal certification (Class C2) for their general purpose network operating system, "NetWare 4." According to IDG's Information Security service research director, "a C2 rating . . . has become a standard for commercial businesses as well as government and military organizations. Customers are using it as a differentiator when making product purchasing decisions." *NetWare 4 Enters Final Phase of C2 Evaluation; On Track to Receive First Client-Server Network Rating*, PR NEWSWIRE, Aug. 28, 1995 (statement of John Pescatore). Susan Biagi argues that commercial-sector security standards are derived from government-published standards. Biagi, *supra* note 52, at 37.

183. *The Trusted Network*, INFOWORLD, Aug. 22, 1994, at 51. C2 ("Controlled Access Protection") is the minimum rating federal agencies must comply with to protect sensitive but unclassified information. For further information on the details of the government's certification rating system, see *supra* note 55.

184. See generally Ellen Messmer, *Gov't Eyes Plans for a Public-Key Infrastructure*, NETWORK WORLD, July 11, 1994, at 8.

185. A "sniffless password" protocol utilizes a "random challenged calculated response method," which transmits a one-time cryptographically-generated password and provides solid identification and authentication. *Reports*, COMPUTER FRAUD & SECURITY BULLETIN, Aug. 1, 1994, 1994 WL 2299920, at *2.

Originators of commercial transactions on the Internet could be required to use an Internet-accessible digital notary system which "automatically detects if electronic documents have been tampered with or backdated."¹⁸⁶ The system can certify that database records, e-mail, word-processing or any other digital documents have not been tampered with by interlopers.¹⁸⁷ The Digital Notary has features such as the "digital fingerprint" and a validation feature.¹⁸⁸ The NSA has tested such a system for its electronic mail system and could require its use in commercial Internet enterprise.

Currently, there are no statutes requiring any of these higher Internet security standards, but this laissez-faire era may soon be over.¹⁸⁹ The creation of higher standards for the commercial sector would likely be a double-edged sword. While assurance of security is crucial to the development and capitalization of the NII, too much risk of liability could impede development.

In the event of the adoption of federal certification, an additional issue will need to be resolved. Some jurisdictions provide that the violation of a statutory rule is only some evidence of negligence in determining whether a defendant exercised due care in the circumstances.¹⁹⁰ Other jurisdictions provide that an unexcused violation of a statute is negligence per se as to consequences that the statute was designed to prevent.¹⁹¹ The probative value of statutory rule violation would need to be harmonized among the jurisdictions.

c. Application of Negligence Doctrine: On-line Service Providers

The rise of commercial on-line service providers such as CompuServe, Prodigy, America Online and Delphi raises novel security liability issues. The primary question is whether a company assumes a greater duty of care when it decides to implement Internet security, as Prodigy Services Co. (Prodigy) was deemed to have done when it screened messages on its "Money Talk" bulletin board.¹⁹²

186. *Internet-Accessible Digital Notary System Detects Electronic Record Tampering*, PR NEWSWIRE, Jan. 17, 1995.

187. *Id.*

188. *Id.*

189. Jared Sandberg, *On Line: Regulators Try to Tame the Untamable On Line World*, WALL ST. J., July 5, 1995, at B1.

190. WILLIAM L. PROSSER, *LAW OF TORTS* 201 (4th ed. 1971).

191. *Id.* at 200.

192. For excellent pre- and post-decision discussions of the *Prodigy* case, see Matthew Goldstein, *Prodigy Case May Solve Troubling Liability Puzzle*, NAT'L L.J., Dec. 19, 1994, at B1; John B. Kennedy et al., *Defamation Law*, NAT'L L.J., July 10, 1995, at B7.

Prodigy, a commercial on-line service provider (OSP), uses software which detects objectionable words and automatically notifies the user that their message will be censored.¹⁹³ After a message accusing Stratton Oakmont, Inc. of fraudulent securities offerings appeared on Prodigy's electronic bulletin board, Stratton Oakmont, filed a defamation lawsuit demanding \$100 million in punitive damages from Prodigy.¹⁹⁴ Prodigy defended on the grounds that it was primarily a passive conduit of information and not a publisher.¹⁹⁵ The district court held Prodigy to the higher standard of a publisher, even though Prodigy did not originate the defamation but only passed it on to its users.¹⁹⁶ The district court stated that, by reviewing and deleting notes from its bulletin boards on the basis of offensiveness, Prodigy "is clearly making decisions as to content... and such decisions constitute editorial control."¹⁹⁷ On October 24, 1995, the *Prodigy* case was settled while the appeal was pending. In an unusual procedural move, Stratton Oakmont agreed to drop its demand for \$100 million damages for defamation in an exchange for Prodigy's apology.¹⁹⁸ Stratton Oakmont also agreed not to contest Prodigy's motion to ask the court to reverse or set aside its previous ruling on Prodigy's status as a publisher.¹⁹⁹ The court's opinion, while unpublished and lacking precedential value,²⁰⁰ nevertheless provides a ready-made line of argument for the next time similar issues arise.

The circumstances of the *Prodigy* dispute raise important legal questions to be addressed in future litigation. If OSPs are to be held to a higher standard of care, and are thus potentially liable for defamation, might they also be liable for misappropriation, invasion of privacy, viruses, stalking, harassment or child pornography on

193. Rex S. Heinke & Heather D. Rafter, *Rough Justice in Cyberspace: Liability on the Electronic Frontier*, COMPUTER LAWYER, July 1994, at 1.

194. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (S.D.N.Y., May 26, 1995) (unpublished decision).

195. *Id.* The *Prodigy* case was critiqued in many electronic discussion groups on the Internet. Professor I. Trotter Hardy stated that sentiment is running "in favor of Prodigy and for unfettered expression on computer bulletin boards." Goldstein, *supra* note 189, at B1 (quoting Professor Hardy). Some courts have been reluctant to find bulletin board operators liable for the torts of their customers. See *Cubby Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (rejecting defamation claim against on-line service on the grounds that it was not a publisher since it exercised no editorial control over the content of statements posted on its bulletin boards).

196. *Prodigy*, 1995 WL 323710 at *10.

197. *Id.*

198. Peter H. Lewis, *After Apology From Prodigy, Firm Drops Suit*, N.Y. TIMES, Oct. 25, 1995, at D1.

199. *Prodigy, Plaintiff Reach Agreement in Libel Case, Deal May Let On-Line Firms Off the Hook*, CHI. TRIB., Oct. 25, 1995, at 3.

200. *Prodigy*, 1995 WL 323710 at *1.

their systems? If an OSP uses security products or technologies to guard against such acts, might the product/technology vendor, licensor, or installer be deemed potentially liable as well, as defendants in an unbroken chain of product distribution? Might liability be more likely to attach if such acts occur due to a security breach? To security laxity? Today, no one thinks twice about dropping sensitive documents, contracts and letters in the mail, though the possibility of theft or destruction, invasion of the correspondents' privacy, or transmittal of defamatory or obscene material exists. If any of these occur, the United States Post Office is not held liable.²⁰¹ Yet the *Prodigy* result may foreshadow a standard whereby an OSP would be held liable for such incidents even though it attempted to deter their occurrence.

The *Prodigy* opinion calibrated the standard of care too high. If that standard is followed, an on-line service that provides hosts to monitor children's chat-areas might find that it has assumed liability of unknown and unknowable magnitude. Despite the *Prodigy* decision's unpublished status, the court's ruling that Prodigy is a publisher casts a cloud of uncertainty over the information highway.

OSPs may be liable for other torts committed by their patrons. For instance, the Clinton Administration's Working Group on Intellectual Property and the National Information Infrastructure has recommended that OSPs be governed by tort law for copyright-infringing materials uploaded to their systems.²⁰² In their final report ("the White Paper"), the Working Group declared that vicarious liability for copyright infringement was appropriate because lowering the liability standard for OSPs would be "a significant departure from current copyright principles and law and would result in a substantial derogation of the rights of copyright

201. The Federal Torts Claims Act provides that claims against the U.S. Postal Service are barred by sovereign immunity. Federal Tort Claims Act, 28 U.S.C. § 2680(b) (1995); *U.S. v. Atlantic Coast Line Ry. Co.*, 215 F. 56 (4th Cir. 1914) (holding the government is not responsible to the owner of mail lost in transit). The U.S. government is deemed to be engaging in a governmental function when it delivers and transports mail. The government is liable to owners of lost or damaged mail only to the extent that it has consented to be liable. *Taylor v. U.S. Post Office Dept.*, 293 F. Supp. 422 (E.D. Mo. 1968); *see also Twentier v. United States*, 109 F. Supp. 406, 124 Ct. Cl. 244 (1953) (holding the United States is liable to the owners of lost and damaged mail only to the extent to which it has consented to be liable and to the extent that liability is defined by the postal laws and regulations).

202. U.S. PATENT AND TRADEMARK OFFICE INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP IN INTELLECTUAL PROPERTY RIGHTS 114 (Final Report, Sept. 5, 1995) (the White Paper).

owners."²⁰³ One reviewer of the White Paper ascribed the Working Group's decision to maintain a high standard for OSPs, in part, to "confidence that advances in encryption, digital cash, digital signatures and other *electronic security mechanisms* will allay the fears of distributors and content owners alike."²⁰⁴

If OSPs can be held liable for infringing material on their services, there is little reason why an Internet service providers (ISP) should not be liable for infringing material uploaded by its customers to Web sites resident on its server computers. ISPs, as well as OSPs, are likely to continue to develop and implement new security technologies in order to compete in the Internet access market. The White Paper indicates that ISPs' increased attention to security will directly impact their liability.

In addition, while OSPs are far from the functional equivalent of Internet security professionals, their activities are inextricably linked and may well become more so in the future as the technologies evolve. Not only may the reliance on Internet security technologies lead to stricter standards for OSPs and ISPs, but Internet security professionals and product makers might also face increasing copyright-related liability as they are asked to deliver increasingly effective on-line security products.

It is not surprising that vicarious tort liability, targeting service providers rather than private individuals, has been the epicenter of conflict over the appropriate role of tort law on the information highway. Individual on-line tortfeasors can avoid repercussions for their actions by simply disguising their messages and postings.²⁰⁵ While this frequently prevents plaintiffs from locating an Internet stalker or other intentional tortfeasor,²⁰⁶ some Internet security products now provide the user with some ability to track tortfeasors or block their access to protected systems.

Licensors of Internet security products could certainly be subject to independent torts arising out of a breach of contract. For example, a licensor of an Internet security product could be subject to the independent tort of fraud or misrepresentation if it marketed a device known to lack the qualities advertised. However, the overarching question is whether new tort doctrines are required to accommodate the new Internet security products. Should the tort law for security products be little more than new wine in old bottles?

203. *Id.*

204. John Kennedy & Mary Rasenberger, *Does Cyberspace Merit a New Legal Order?*, N.Y. L.J., Oct. 4, 1995, at 1 (emphasis added).

205. Branscomb, *supra* note 153, at 1643.

206. *Id.*

For the licensor of nationally-marketed security products, there is the additional problem of whose tort law applies. Tort law is traditionally state law and thus there are fifty different tort regimes. The problem is compounded by the internationalization of the sale of security products.²⁰⁷ Internet security products are not only sold within the continental United States, they are distributed to more than 100 countries via the Internet.

As this discussion demonstrates, common law tort doctrine is an inefficient means of allocating risk in the Internet security market. At this point in time, there is little case law or commentary applying negligence theory to computer software and service providers. As reliance on Internet security technologies increases, it becomes more important to protect and encourage security software and related service providers in the market. Reliance on nonexistent, inconsistent or vague standards of negligence liability could defeat this goal.

2. STRICT PRODUCTS LIABILITY

Products liability generally refers to legal liability of manufacturers for injuries caused by the marketing of products. Strict products liability grew out of a societal judgment "that people need more protection from dangerous products than is afforded by the law of warranty."²⁰⁸ Basically, strict products liability permits an injured consumer to recover damages for physical injury or property damages from a manufacturer upon a showing that the manufacturer distributed

207. Tort law presents intractable problems of conflicts of law. The first reported appellate opinion applying defamation in Cyberspace was the Australian case of *Rindos v. Hardwick*, No. 1994 of 1993 (W. Austl. Sup. Ct. Mar. 31, 1994) (discussed in Geoff Thomas, *\$40,000 Awarded in First Cyberspace Defamation Case*, AUSTRALIAN FINANCIAL REVIEW, May 4, 1994 (available on LEXIS, AUST Library, AUSNEWS file)). In *Rindos*, an Australian anthropologist allegedly defamed a fellow Australian anthropologist on the Internet, accusing him of engaging in pedophilia and of being professionally incompetent. The Supreme Court of Western Australia awarded the plaintiff \$40,000, the largest defamation award in the past four years.

The *Rindos* case highlights the frailties of applying tort law to redressing conflicts on the Internet. Suppose the defamatory communications had crossed international borders? Suppose the anthropologist had been defamed, not by a fellow Australian, but by a citizen of Saudi Arabia? Would the anthropologist really have a reputational interest in Saudi Arabia? If the anthropologist were a person of some fame, could the Saudi defendant rely upon the doctrine of limited public figure, which is an American rule? The problem of jurisdiction is another problem with tort law. What jurisdiction would apply? The jurisdiction of where the alleged defamation arose, or where it was received? Contract law, in contrast, permits the parties to chose a forum state so long as it bears a reasonable relationship to the contract or the parties.

208. *East River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 866 (1986).

a product²⁰⁹ containing a dangerous defect²¹⁰ into the stream of commerce, and that the defective product caused the injury.²¹¹ Neither negligence nor privity must be proved.²¹² The vast majority of American jurisdictions have adopted this standard over the past thirty years.²¹³

Strict products liability would pose great advantages for purchasers damaged by Internet or Internet security products. For example, strict products liability offers recourse to third parties who would be excluded from breach of contract actions due to lack of privity. Additionally, buyers avoid the notice requirement and are shielded from vendor-imposed liability limitations that are part and parcel of the U.C.C.²¹⁴

209. The Third Circuit has held that when computer programs are "implanted in a medium," they are "tangible, moveable" and become "products." *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670, 675-76 (3d Cir. 1991). If an Internet security measure were deemed not to be a "product," strict products liability could not apply. *See, e.g., Salomey v. Jeppesen & Co.*, 707 F.2d 671, 676-77 (2d Cir. 1983) (rejecting argument that producing navigation charts is a service and holding they are products for purposes of Restatement § 402A); *Aetna Casualty & Sur. Co. v. Jeppesen & Co.*, 642 F.2d 339, 342-343 (9th Cir. 1981) (holding navigation charts to be products).

210. RESTATEMENT (SECOND) OF TORTS § 402A (1964).

211. The plaintiff need only establish that a defect in software proximately caused injury or damage to recover in strict products liability. *See generally* Diane B. Lawrence, *Strict Liability, Computer Software and Medicine: Public Policy at the Crossroads*, 23 TORT & INS. L.J. 1 (1987). For a discussion of Internet security products see *infra* part II.B.

212. RESTATEMENT (SECOND) OF TORTS, § 402A (1964).

213. Most jurisdictions have adopted some version of § 402A of the *Restatement (Second) of Torts*, which states:

Special Liability of Seller of Product for Physical Harm to User or Consumer

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

(a) the seller is engaged in the business of selling such a product, and

(b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

(2) The rule stated in Subsection (1) applies although

(a) the seller has exercised all possible care in the preparation and sale of his product, and

(b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.

RESTATEMENT (SECOND) OF TORTS § 402A.

214. The U.C.C. will be discussed in detail in the *infra* part III.B. The U.C.C. requires buyers to give notice of defects to sellers. U.C.C. § 2-607(3)(a) (1990). Section 2-719 allows vendors to limit damages and remedies, but places constraints on the extent of limitation:

Thomas Wolpert posits possible scenarios where failed software²¹⁵ may be unreasonably dangerous or "place life and limb in peril."²¹⁶ The hypothetical situations involve:

An energy management system in a high school that was programmed to be inoperable until 6:30 a.m. and that prevented an exhaust fan in a chemistry lab from working, thus causing a teacher to inhale chlorine gas.

A computer system that generated a warning label for a prescription drug that was inadequate and that the pharmacist failed to use anyway.

A computer system used by a pretrial service agency that failed to warn an arraignment judge that an arrestee was out on bond for two previous armed robberies, a circumstance that resulted in the release of the arrestee and grave injuries to a person wounded in another armed robbery attempt.

A defective computer and software program that were used to assist in calculating doses of radiation received for patients who were being seeded with radioactive implants to treat cancer of the prostate.²¹⁷

The policy interest in preventing "the marketing of products having defects that are a menace to the public" is strong.²¹⁸ The manufacturer, even if not negligent in the manufacture of the product, is best situated to prevent such products from reaching the market, and bears the risk of such occurrences.²¹⁹ Given this policy, the above cases would seem appropriate for strict products liability treatment. Some commentators favor extending strict liability to defective software where personal injury is the result.²²⁰

(2) Where circumstances cause an exclusive or limited remedy to fail of its essential purpose, remedy may be had as provided in this Act.

(3) Consequential damages may be limited or excluded unless the limitation or exclusion is unconscionable. Limitation of consequential damages for injury to the person in the case of consumer goods is prima facie unconscionable but limitation of damages where the loss is commercial is not.

U.C.C. § 2-719 (1990).

215. Wolpert, *supra* note 173, at 519.

216. Products liability grew out of this famous statement made by Judge Cardozo in *MacPherson v. Buick Motor Co.*, 111 N.E. 1051, 1053 (N.Y. 1916).

217. Wolpert, *supra* note 173, at 519.

218. *Escola v. Coca Cola Bottling Co. of Fresno*, 150 P.2d 436, 441 (Cal. 1944) (concurring opinion).

219. *Id.*

220. See, e.g., Brannigan & Dayhoff, *supra* note 162, at 130; Susan Lanove, *Computer Software and Strict Products Liability*, 20 SAN DIEGO L. REV. 439, 456 (1983); Patrick T.

While courts have decided that products liability can apply to manufacturers of defective computer programs,²²¹ they have been reluctant to actually extend strict products liability to computer software.²²² Wolpert observes that strict products liability actions have "been slow to develop against the vendors of software."²²³ Given this reluctance, it seems unlikely that courts would apply strict products liability to defective Internet security products which injure only property.²²⁴

Where the only damage is to the Internet security product, courts would likely apply warranty law, rather than strict products liability. In *East River Steamship Corp. v. Transamerica Delaval, Inc.*,²²⁵ the United States Supreme Court refused to apply strict products liability in admiralty in a case where the only loss was to the product itself. The Court reasoned that contract and warranty law were better suited to deal with commercial losses than was strict products liability. The Court stated that if products liability were extended too far, "contract law would drown in a sea of tort."²²⁶

3. DEFENSES

The history of tort law has been characterized by the creation of defenses and immunities from legal liabilities.²²⁷ In the nineteenth

Miyaki, *Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121 (1992).

221. See, e.g., *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D. N.J. 1979), *aff'd*, 635 F.2d 1081 (3d Cir. 1980).

222. See *id.*

223. Wolpert, *supra* note 173, at 519. Most commentators contend that strict liability should not apply to defective software, since computer software is predominately a service. See, e.g., Roy N. Freed, *Products Liability in the Computer Age*, 17 JURIMETRICS J. 270 (1977).

224. In the course of strict products liability evolution, a manufacturer's duty of care was broadened to include protection against property damage. See *Marsh Wood Prods. Co. v. Babcock & Wilcox Co.*, 240 N.W. 392, 399 (Wis. 1932); *Genesee County Patrons Fire Relief Assn. v. L. Sonneborn Sons, Inc.*, 189 N.E. 551, 553-55 (N.Y. 1934). A majority of courts have held that such damage has to be to property other than the defective product itself. See *Seely v. White Motor Co.*, 403 P.2d 145 (Cal. 1965); *Jones & Laughlin Steel Corp. v. Johns-Manville Sales Corp.*, 626 F.2d 280, 287 & n.13 (3rd Cir. 1980). A minority of courts have held that strict liability may encompass cases where the only property damage is to the defective product itself. See *Emerson G.M. Diesel, Inc. v. Alaskan Enterprise*, 732 F.2d 1468, 1474 (9th Cir. 1984) (declining to follow *Seely*); *Santor v. A. & M. Karagheusian Inc.*, 207 A.2d 305, 312-13 (N.J. 1965) (finding manufacturer liable where only loss was to defective carpeting).

225. 476 U.S. 858 (1986).

226. *Id.* at 866.

227. See MORTON J. HORWITZ, *THE TRANSFORMATION OF AMERICAN LAW 1780-1860*, 99-161 (1977).

century, courts carved out doctrines such as the fellow-servant rule, assumption of risk and contributory negligence to mitigate or absolve a defendant's wrongdoing. Morton Horwitz argues that the origin of these defenses served as a subsidization of economic growth for the developing industrialization.²²⁸ Such defenses would undoubtedly be raised in the realm of Internet security breach as well.

Perhaps, just as there may have been legal subsidies for economic development in the nineteenth century, courts could encourage the development of the NII by employing these legal doctrines to guarantee certainty and predictability of economic consequences today.²²⁹ During the early years of the NII, there may be a need to afford legal subsidies to those who capitalize the Internet. On the other hand, such subsidies could leave victims of devastating security breaches with no redress. For example, if a firewall were even inadvertently misused, the vendor of the firewall could assert product misuse and potentially escape liability. Or, if a company's network was illicitly entered from the Internet by a novel means after an Internet security consultant had been hired to recommend and assist in the implementation of hacker-proof security policies and products, the company's remedy could evaporate if the consultant could show the method of invasion was reasonably unforeseeable.

Moreover, courts would need to determine if damages would be affected when a victim of an Internet security breach fails to take "reasonable precautions." For example, most computer industry experts agree that the only secure passwords are ones that are a *minimum* of seven randomly-chosen letters, numbers and symbols.²³⁰ The shorter the password, the easier it is to crack. Thus, passwords that are too short or do not meet other criteria may invite the defense of contributory negligence.

As early as 1993, one Internet security expert declared that any password chosen in accordance with any of the following methodologies is insecure:

1. Modifying any part of your name or name plus initials;
2. Modifying a dictionary word;
3. Acronyms;
4. Any systematic, well-adhered-to algorithm. For instance,

228. *Id.*

229. *Id.* at 111.

230. *See, e.g.*, A LEC MUFFET, ALMOST EVERYTHING YOU EVER WANTED TO KNOW ABOUT SECURITY* (*BUT WERE AFRAID TO ASK!), Security.FAQ, version 2.2, Dec. 3, 1993, available at "ftp://coast.cs.purdue.edu/pub/doc/faq/faq-security.txt.z" on the World Wide Web.

never use passwords like: alec7 (it's based on the user's name (and it's too short anyway); tteffum (based on the user's name again); gillian (girlfriend's name—in a dictionary); naillig (ditto—backwards); PORSCHE911 (it's in a dictionary); 12345678 (it's in a dictionary and people can watch you type it easily); qwertyui (ditto); abcxyz (ditto); Oooooooooo (ditto); Computer (just because it's capitalized doesn't make it safe); wombat6 (ditto for appending some random character); 6wombat (ditto for appending some random character); nerde3 (even for French words); mr. spock (it's in a sci-fi dictionary); zeolite (it's in a geological dictionary) ze0lite (corrupted version of a word in a geological dictionary); ze01lte (ditto); Z30L1T3 (ditto).²³¹

The security expert concluded: "[T]hese examples emphasize that ANY password derived from ANY dictionary word (or personal information), modified in ANY way, constitutes a potentially guessable password."²³² With the increasing awareness of the importance of password security, judges may have little difficulty finding companies contributorily negligent if they do not bother to implement and adhere to acceptable password security recommendations. Soon, it may be contributorily negligent for a firm to permit any remote access to a router/gateway which is not protected by one-time passwords.

To further underscore the unwieldy nature of liability allocation by negligence law, consider the following scenario. Suppose a minor bypasses Internet security controls and is stalked by a pedophile on the Internet. Would the minor be found contributorily or comparatively negligent on the grounds that when a legal infant performs an adult activity, he is held to an adult standard of care? Would a minor's contributory negligence be imputed to the parent? Is surfing the Internet the functional equivalent of performing an adult activity, such as operating an automobile, airplane, snowmobile or powerboat? More generally, would the failure of a user to look out for his own security bar him from recovery for damages or expose him to suit by others?

Answers to questions such as these and the related issues discussed above will take years to be worked out in the courts. Using traditional tort doctrine to allocate liability for failed Internet security products raises as many questions as it answers. While tort law will have its place in Cyberspace, it is apparent that it fails as a primary framework for "regulating" Internet security products. Tort law cannot readily provide resolutions to the issues above. This

231. *Id.*

232. *Id.*

leaves manufacturers, vendors, consultants and users of Internet security products unsure where they stand with respect to liability. A more certain framework is desirable so that the growth of the NII will not be impeded by uncertainty in the law. Given the drawbacks of a tort law paradigm, we turn to an examination of contract principles and their potential efficacy in affording a workable framework for allocation of liability with respect to failed Internet security products.

B. Regulation Under Current Contract Law

Contract law is the principal mechanism for facilitating market transactions.²³³ Since contract law permits "individuals to pursue their voluntary choices,"²³⁴ several commentators argue that contract law provides the legal ground rules of the Internet.²³⁵ This part examines the appropriateness of contract law as a general framework for allocating the risks and liabilities that arise out of commercial transactions involving Internet security products. First, we survey the effectiveness of applying traditional contract theory. Then we examine the application of U.C.C. Article 2 sales principles to Internet security product transactions.

1. TRADITIONAL NOTIONS OF CONTRACT LAW

Modern contract law has its roots in the nineteenth century philosophy of the freedom of contract. Under this view, parties had broad freedom to make their own voluntary arrangements, and the courts' role was to interpret and enforce the parties' obligations by employing the principles of liberty, equality and reciprocity, the dominant values of a market economy.²³⁶ Contract law provided the means to permit parties to strike the deal they truly wanted, within the parameters of good faith and fair dealing, rather than a deal prescribed by some centralized authority.²³⁷ Yet, total freedom of contract allowed one contracting party to oppress the other whenever asymmetrical relationships of power and economic position between

233. See JOHN TILLOTSON, *CONTRACT LAW IN PERSPECTIVE* 3 (1981).

234. HUGH COLLINS, *THE LAW OF CONTRACTS* 1 (1986).

235. See generally Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 *JURIMETRICS J.* 1 (1994); Hardy, *supra* note 29; David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 *VILL. L. REV.* 487 (1993).

236. COLLINS, *supra* note 234, at 9.

237. JOHN COLLINGE, *TUTORIALS IN CONTRACT* 10-14 (1981).

the two parties existed.²³⁸ While classical contract theory ignored the law's role in legitimizing the position of the well-off who enjoy great power in the market,²³⁹ there has been a counter-movement in modern contract theory moderating the harsh consequences that stem from unequal bargaining power.²⁴⁰ Frederick Kessler's classic law review article addressed the problem of how courts should treat contracts where the lesser party is required to adhere to the terms of the stronger.²⁴¹ The lesser party is protected to a certain extent from being forced to comply with unfair terms of a contract by the application of the doctrine of unconscionability.²⁴² To this end, modern courts have increasingly scrutinized the underlying fairness of the contract where the parties are in vastly different bargaining positions.²⁴³

Modern contract law retains the flexibility and malleability of traditional contract theory. Since contract law enables the parties to forge unique solutions to emergent legal problems, it is particularly well suited for the new information technologies.²⁴⁴ Contract law's capacity to evolve as a voluntary social institution is in contrast with the coercive features of tort law. General contract law principles fit well with the emergent culture of the Internet, which eschews involuntary obligations, whether imposed from the state or from tort law. Commentators suggest that contract law, unlike tort (and criminal) law, is ideally situated to informally regulate unauthorized Internet access and hacker malfeasance.²⁴⁵ For instance, Robert Dunne believes that contract law conforms to the original Cyberians'

238. *Id.* at 11.

239. Professor Stewart Macaulay and his University of Wisconsin colleagues critique the law and economics idealization of contract theory as turning a blind eye to the ways that contract law legitimates and validates the position of the powerful and wealthy in society. STEWART MACAULAY, *CONTRACTS: LAW IN ACTION* 10 (1995). They note that the law and economics approach to contract theory fails to "deal with the justice or fairness of the present distribution of wealth, status, privilege or power in the society." *Id.*

240. See generally COLLINS, *supra* note 234.

241. Frederick Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

242. Arthur Leff subdivided the doctrine of unconscionability into procedural unconscionability (unfairness in striking a bargain) and substantive unconscionability (unfairness in the terms of the bargain itself). Arthur A. Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485 (1967).

243. COLLINS, *supra* note 234, at 67.

244. The abolition of the institution of imprisonment for breach of contract and the rise of compensatory principles in contract law were two key developments in modern contract law. See A.W.B. SIMPSON, *A HISTORY OF THE COMMON LAW OF CONTRACT* 601-02 (1975).

245. See Dunne, *supra* note 235, at 1.

aversion to centralized management and respects their desire for mutually-agreed-upon norms.²⁴⁶ Trotter Hardy also argues that the self-regulation aspect of contract law offers legal solutions for many legal issues arising in Cyberspace.²⁴⁷ He concludes:

[T]he rapidly changing technology of computer communications implies a need for flexible legal regulation of behavior, and that flexible regulation in turn implies a presumption that the most decentralized rules should be applied whenever possible. This will often entail contractual agreements worked out among the affected parties, rather than a broadly-applicable judicial or legislative resolution.²⁴⁸

The new information technologies are already employing contract law in the transnational space of the electronic frontier.²⁴⁹ David Johnson and Kevin Marks advocate "primary reliance on contracts to govern the Cyberspace environment."²⁵⁰ With respect to on-line service providers and consumers, these commentators maintain that contract law effectively governs key aspects of their relationships,²⁵¹ and that the "marketplace provides adequate incentives for all concerned to agree on the rules, once the general need for choice in the face of a flexible electronic environment is understood."²⁵²

Contract law, however, has limitations. For instance, contract law does not effectively address liability for injuries to third parties. While a licensor and licensee are free to contract, they are not free to discharge their legal obligations to unknown third parties injured by the failure of Internet security products. Accordingly, there will be a residual role for tort law when a third party is injured as the result of the failure of a security product. These third-party injuries may be economic or non-economic. For example, the Veterans Health Administration has a computer network including "172 medical centers, 350 outpatient clinics and 130 nursing homes nationwide."²⁵³ A doctor or other health practitioner in such a networked medical environment may be liable for permitting disclosures of confidential

246. See *id.* at 10-11.

247. See Hardy, *supra* note 29, at 995.

248. *Id.* at 995-96.

249. See Saskia Sassen, *Interdisciplinary Approaches to International Economic Law: When the State Encounters a New Space Economy: The Case of Information Industries*, 10 AM. U. J. INT'L L. & POL'Y 769, 772 (1995).

250. Johnson & Marks, *supra* note 235, at 489-90.

251. See *id.* at 490.

252. *Id.* at 514.

253. Silver, *supra* note 53, at 71.

patient information.²⁵⁴ Also, a bank may be liable for a security breach that results in confidential financial information being disclosed to a competitor or intruder.²⁵⁵

In addition to dealing with third-party issues, contract law in the digital age requires a specialized paradigm for dealing with the unique issues of contract formation, interpretation, performance, warranties and remedies. In particular, specialized ground rules for dealing with the transfer of rights in information technologies are needed. We next turn to the U.C.C. as a possible paradigm for resolving these issues.

2. CURRENT UNIFORM COMMERCIAL CODE

In this part, we argue that the U.C.C.'s Article 2 sales doctrine should not be applied to Internet security product transactions because it is fundamentally inconsistent with the commercial reality of such transactions.²⁵⁶ The goal of the U.C.C. is to forge and employ default rules that reflect commercial reality and balance the interests of diverse stakeholders in commercial transactions.²⁵⁷

a. Overview

The U.C.C. as a whole is "a single subject of law" that deals "with all of the phases which ordinarily arise in the handling of a

254. The release of confidential patient records violates the fiduciary relationship between physician and patient. Many states have statutes limiting the disclosure of a patient's health care information. See, e.g., California Confidentiality of Medical Information Act, CAL. CIV. CODE § 56 (1981) (defining circumstances under which health information may be disseminated to third parties); MONT. CODE ANN. § 50-16-501 (1987) (providing rules for disclosures of patient's health care information). Wrongful disclosure of patient records may also be the basis of tort actions based upon invasion of privacy, breach of fiduciary duty and the intentional infliction of emotional distress. See, e.g., *Banks v. Charter Hosp. of Long Beach*, 1992 WL 521069 (LRP Jury) (punitive damages awarded under an invasion of privacy action to a plaintiff who suffered emotional distress when her name and photograph appeared in an article about the defendant hospital without her consent); *Austin v. Methodist Hospital*, 1987 WL 231638 (LRP Jury) (awarding compensatory and punitive damages for unauthorized release of plaintiff's medical records of the strictest confidential nature). See also Annotation, *State Statutes or Regulations Expressly Governing Disclosure of Fact That Person Has Tested Positive for Human Immunodeficiency Virus (HIV) or Acquired Immunodeficiency Syndrome (AIDS)*, 12 A.L.R. 5th 149 (1994).

255. See generally Edward L. Raymond, Jr., Annotation, *Bank's Liability Under State Law, for Disclosing Financial Information Concerning Depositor or Customer*, 81 A.L.R. 4th 377 (1994).

256. Contract law generally requires a legal infrastructure advancing commercial practices. See Charles J. Goetz & Robert E. Scott, *The Limits of Expanded Choice: An Analysis of the Interaction Between Express and Implied Contract Terms*, 73 CAL. L. REV. 261 (1985).

257. U.C.C. §§ 1-102(1), (2) (1990).

commercial transaction."²⁵⁸ The goals of the U.C.C. were "to simplify, clarify and modernize the law governing commercial transactions."²⁵⁹ The U.C.C. was also intended "to permit the continued expansion of commercial practices through custom, usage and agreement of the parties."²⁶⁰

The U.C.C.'s overarching comprehensiveness can be illustrated by analyzing a commercial transaction. Imagine a sale of turkeys by a Minnesota farmer to the Big Super Market chain in Massachusetts. If the farmer is defined as a merchant, his turkeys must meet certain minimum quality standards, even if he makes no representations regarding the quality of his turkeys. If the turkeys never arrive at Big Super's loading dock, Big Super may have seller's remedies under Article 2. In the event of Big Super's default, the farmer might obtain an Article 9 security interest in the turkeys. The check issued by Big Super's manager in payment would be covered by Article 3 of the U.C.C. governing negotiable instruments. If the farmer deposits the check into his bank account, Article 4, which deals with the collection of checks and the relationship between the bank and the customer, is triggered. If the goods are stored or shipped, they may be covered by a bill of lading or warehouse receipt under Article 7. The U.C.C. deals with all of the stages in the life of a commercial transaction—from cradle to grave.

U.C.C. Article 2 is consistent with freedom of contract because it permits buyers and sellers to vary most provisions by agreement.²⁶¹ However, the parties are not free to disclaim "the obligations of good faith, diligence, reasonableness and care" ²⁶² The U.C.C. serves as a default model, supplying "gap-filler" contract terms for those the parties do not negotiate.²⁶³ Using the U.C.C. is analogous to buying a suit "off the rack." The alternative is to have a suit tailored to your specific body dimensions. Article 2 is composed of default or "off the rack" contract terms. If the parties are dissatisfied with Article 2's

258. U.C.C. pmb. (1990).

259. U.C.C. § 1-102(2)(a) (1990).

260. U.C.C. § 1-102(2)(b) (1990).

261. See U.C.C. § 1-102 Official Comt. 2 (1990) (stating that "freedom of contract is a principle of the [U.C.C.]"). The U.C.C.'s freedom of contract is tempered by the concepts of good faith and commercial reasonableness that permeate the statute. Section 1-203, for example, provides that "[e]very contract or duty within [the U.C.C.] imposes an obligation of good faith in its performance or enforcement." See generally Dennis M. Patterson, *Wittgenstein and the Code: A Theory of Good Faith Performance and Enforcement Under Article Nine*, 137 U. PA. L. REV. 335 (1988).

262. U.C.C. § 1-102(3) (1990).

263. See U.C.C. §§ 2-304 to -310 (1990).

default terms, they are always free to tailor their own sales contract solution.

b. Application of U.C.C. Article 2 to Internet Security Products and Services

Robert Feldman notes that "the information age is working profound changes in every area of the law."²⁶⁴ Sales law and licensing law have not escaped this influence.²⁶⁵ This part examines how the emerging information technologies pose new challenges for traditional sales law.

A contract for the sale of goods is one in which a seller agrees to transfer goods that conform to the contract in exchange for valuable consideration.²⁶⁶ Article 2 of the U.C.C. applies to "transactions in goods."²⁶⁷ There are some questions whether Internet security products are 'goods' within the scope of Article 2. Internet security products typically consist of or incorporate software. "Software" is defined in a proposed revision of the U.C.C. as "a computer program in source code, object code or in any other form, together with any associated data, program description, media and supporting documentation."²⁶⁸ Software may have a tangible aspect to the extent that it resides in various forms of media, but it also has intangible attributes which allow it to change form and appearance like a chameleon. Software is typically licensed, not sold; like Internet security products, it is transferred by a combination of sales/licensing transaction.²⁶⁹ Software is also intellectual property, subject to the regime of federal statutory law.²⁷⁰

Software is already treated as within the scope of U.C.C. Article 2 by the vast majority of courts. Some courts struggle with the intangible qualities of software, applying the U.C.C. by analogy.²⁷¹ Generally, courts distinguish between "sales" and "services": The former is governed by Article 2 whereas the latter falls under the

264. Robert A. Feldman, *A New Draft of UCC Article 2: A High Tech Code Takes Form*, 12 *COMPUTER LAW* 1 (Feb. 1995) [hereinafter Feldman, *New Draft*].

265. *Id.*

266. U.C.C. § 2-301 (1990).

267. U.C.C. § 2-102 (1990).

268. U.C.C. § 2-104(43) (Proposed Draft, Feb. 10, 1995).

269. This commercial reality is reflected in the Internet security product "sales and license agreement" reproduced in Appendix A, *infra*.

270. See generally 17 U.S.C. §§ 101-1101 (1994) (copyright); 35 U.S.C. §§ 1-376 (1988 & Supp. 1993) (patent).

271. Herbert J. Hammond, *Limiting and Dealing With Liability in Software Contracts*, 9 *COMPUTER LAW* 22 (June 1992).

auspices of the common law.²⁷² Courts look to the "predominant purpose" of a software agreement to determine which law should be applied.²⁷³ In light of this distinction, a difficult question concerns vendors who install software security products *and* have continuing service obligations.²⁷⁴

If Article 2 applies, a vendor of security products who claims his products to be "hacker-proof," "bullet-proof" or "air tight" could be subject to the express warranty obligations of the U.C.C.²⁷⁵ A vendor, however, could argue that these statements are mere sales talk or "puffing" and not definite enough to constitute warranties.²⁷⁶ Despite the damage to the buyer's intellectual property,²⁷⁷ courts customarily apply the U.C.C. rather than strict products liability to faulty software claims.

272. The bifurcated treatment of sales and services was first conceived centuries ago in the law-merchant tradition. See *Milau Assocs., Inc. v. North Ave. Dev. Corp.*, 368 N.E.2d 1247 (N.Y. 1977).

273. With hybrid transactions involving both sales and service, only transactions which are predominately sale of goods are within Article 2. If a court determines that services predominate, common law principles apply. See *Micro-Managers, Inc. v. Gregory*, 434 N.W.2d 97, 100 (Wis. Ct. App. 1988) (holding that under the predominant factor test, contract to develop software was not subject to U.C.C. because it was for services not goods); *Bonebrake v. Cox*, 499 F.2d 951, 960 (8th Cir. 1974) (holding that for a mixed contract, test is whether predominant factor, thrust and purpose is rendition of services).

Some courts are now applying William Hawkland's "gravamen" test. E.g., *Anthony Pools v. Sheehan*, 455 A.2d 434 (Md. 1983) (applying gravamen test to mixed sales and service transaction involving inground swimming pool with diving board). Dean Hawkland defines the gravamen test as follows:

Unless uniformity would be impaired thereby, it might be more sensible and facilitate administration, at least in this grey area to abandon the "predominant factor" test and focus instead on whether the gravamen of this action involves goods or services. For example, in *Worrell v. Barnes*, if the gas escaped because of a defective fitting or connector, the case might be characterized as one involving the sale of goods. On the other hand, if the gas escaped because of poor work by Barnes the case might be characterized as one involving services, outside the scope of the U.C.C.

I.W. HAWKLAND, UNIFORM COMMERCIAL CODE SERIES § 2-102:04 at Art.2, at 12 (1982); see also PETER B. MAGGS ET AL., *COMPUTER LAW: CASES, COMMENTS, QUESTIONS* 386 (1991).

274. There is little case law or commentary on applying warranties to services. See Robert A. Feldman, *Warranties and Computer Services: Past, Present and Future*, 10 *COMPUTER LAW* 1 (Feb. 1993) [hereinafter Feldman, *Warranties*].

275. U.C.C. § 2-313 (1990).

276. Express warranties are provided for under U.C.C. § 2-313, the implied warranty of merchantability under U.C.C. § 2-314, and the implied warranty of fitness for a particular purpose under U.C.C. § 2-315.

277. See generally Wolpert, *supra* note 173.

In addition, under the Article 2 sales regime, Internet security vendors could be subject to implied warranties of quality. To establish a breach of an implied warranty of merchantability, for example, the plaintiff would need only prove that an Internet security product was not merchantable²⁷⁸ at the time of sale (or licensing) and that injury or damage was caused proximately, and in fact, by the security product.²⁷⁹ Therefore, the failure of an Internet security product to prevent a hacker from entering a computer could potentially be actionable under an implied warranty if it could be proved that the security device was below the standard of other security products on the market.

On the other hand, the U.C.C. allows vendors to disclaim implied warranties, limit their liability and restrict buyers' remedies within the parameters of good faith, commercial reasonableness and conscionability. The extent to which vendors could use such disclaimers and limitations of liability to reallocate contract liability in Internet security contracts is unclear. Section 2-719 permits parties to set their own remedies and measure of damages.²⁸⁰ Internet security vendors often provide an "exclusive remedy" in lieu of remedies normally available under the U.C.C.²⁸¹ The vendor of a pre-packaged firewall product might attempt to limit liability to the "exclusive," but limited remedy of repairing or replacing the equipment and software.²⁸² Where the court finds the provision to be unconscionable, however, a network security vendor is neither free to agree upon an "exclusive" but nugatory remedy nor permitted to limit or exclude consequential damages.²⁸³ The court will not enforce a remedy that "fail[s] of its essential purpose."²⁸⁴ Thus, the sole remedy of repairing or replacing the Internet security software might not be enforced. If a court refuses to enforce such provisions, the aggrieved buyer will have the full panoply of Article 2 remedies at

278. "Merchantable goods" are those which "at least (a) pass without objection in the trade under the contract description . . . and (c) are fit for the ordinary purposes for which such goods are used . . . and (f) conform to the promise or affirmation of fact made on the container or label if any." U.C.C. § 2-314(2) (1990).

279. U.C.C. §§ 2-714, 715 (1990).

280. U.C.C. § 2-719 (1990).

281. U.C.C. § 2-719(1)(b) (1990).

282. See generally DeLois T. Leapheart, *Contractually Limiting Liability*, 72 MICH. BUS. L. J. 546 (1993); Note, *U.C.C. Section 2-719: Limited Remedies and Consequential Damage Exclusion*, 74 CORNELL L. REV. 359 (1989); Roy Ryden Anderson, *Contractual Limitations of Remedies*, 67 NEB. L. REV. 548 (1988). See also *infra* App. A §14(b).

283. U.C.C. § 2-719(3) (1990).

284. U.C.C. § 2-719(2) (1990).

her disposal.²⁸⁵ If the disclaimers are enforced, the licensee would be allocated the costs of the security breach. A licensee would then bear the costs of all tort and statutory actions based upon unexcused disclosures of confidential information.

Article 2 not only fails to provide answers to the complex contracting questions posed by software transactions, but also fails to resolve the basic question: Is the licensing of software the sale of a "good" covered by U.C.C.²⁸⁶ or a "service"? The U.C.C. has not enabled the modernization of commercial law pertaining to software, Internet security products and other intangibles. At present, vendors of Internet security products lack an accessible and determinate body of law.²⁸⁷

3. ARTICLE 2 SALES VERSUS LICENSING OF INTANGIBLES

Judges and practitioners find Article 2 inadequate when it comes to the new information technologies.²⁸⁸ It is doctrinally inconsistent for Article 2 to cover both the "sale of tangibles" and the "licensing of intangibles." Article 2 of the U.C.C. deals with the *sale of tangible goods*; network security products typically involve the *licensing of intangibles*.

A "sale" is defined by the "passing of title from a seller to a buyer for a price."²⁸⁹ In transactions governed by Article 2, title passes from buyer to seller.²⁹⁰ In contrast, title typically does not pass in the licensing of an Internet security product. Rather, licensing is a lower-order transfer of property interest conveying a right to use electronic information and other intangibles for a designated period of time or under designated conditions. The licensing of intangibles, like

285. U.C.C. § 2-719 (1990).

286. Bonna Lynn Horovitz, Note, *Computer Software As a Good Under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth*, 65 B.U. L. REV. 129 (1985).

287. Karl N. Llewellyn, *Why We Need the Uniform Commercial Code*, 10 U. FLA. L. REV. 367, 369 (1957) (explaining the purpose of the U.C.C. as a codification project to promote accessibility and efficient commercial transactions).

288. See generally Jonathan Groner, *This Uniform Code Does Not Compute: Software Industry Balks at Rewrite of Commercial Law*, LEGAL TIMES, Nov. 1, 1993, at 1 (contending that the ground has moved under the present version of Article 2 for all software licensing transactions).

289. U.C.C. § 2-106(1) (1990).

290. Section 2-401(1) provides that "title to goods passes from the seller to the buyer in any manner and on any conditions explicitly agreed on by the parties." U.C.C. § 2-401(1) (1990).

leases, validates the right to use all forms of intellectual property.²⁹¹ While the essence of a sale is the passing of title for a price,²⁹² with intangibles, the passing of title is only a vehicle for conveying valued intellectual property and the right to use that information.²⁹³ The title to tangible copies of intangibles is not dispositive or even relevant to any software licensing rights.²⁹⁴ The medium is not the message,²⁹⁵ only the right to exploit information.

An intangible may consist of data, information, software or intellectual property rights. Under Article 2, a buyer may freely assign her rights in the goods. In contrast, the typical security software license prohibits assignment and may have other use restrictions. Diagram One illustrates in tabular form the differences between a typical sales transaction and the licensing of security software.

291. Consumer finance leases are regulated by Article 2A of the U.C.C. Leases grant the limited right to use goods, whereas licenses are a limited right to use intangibles.

292. U.C.C. § 2-106(1) (1990).

293. See generally Steven O. Weise, *Article 9—Personal Property Secured Transactions*, 46 BUS. LAW. 1711 (Aug. 1991).

294. Robert Mitchell argues that the proposed U.C.C. § 2-2501(a) might state that "title to goods or tangible copies is not dispositive or relevant to any issue addressed in this chapter." See Memorandum from Robert B. Mitchell, Task Group Co-Leader to Donald A. Cohn & Ellen Kirsh, Co-Chairs, ABA Software Subcommittee, Business Law Section, American Bar Association, Parts 21 & 23 (Mar. 3, 1995) (on file with the *High Technology Law Journal*).

295. Marshall McLuhan's famous aphorism about television was that the "medium is the message." MARSHALL MCLUHAN, *UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN* 7 (1964). The medium in a licensing transaction is the diskette or other tangible vehicle. The proposed licensing chapter applies to the tangible copies of the intangible property leaving the rules for transferring intangibles to federal intellectual property law. See U.C.C. § 2-2501(a) (Proposed Draft, Feb. 10, 1995).

DIAGRAM ONE: LICENSING VERSUS SALES

Attribute	Licensing	Sale
Transfer of Title	Mass-marketed security products are typically licensed. No title passes. Customized Internet security transactions often involve the sale of hardware, the licensing of software and the procurement of services.	Title to goods passes when the buyer accepts and pays in accordance with the contract. U.C.C. § 2-301.
Use Restrictions	Location and use restrictions are typically specified in the license agreement.	Once title passes, typically no location or use restrictions exist in the sale of goods.
Norm of Confidentiality	Licensee is typically not permitted to resell or transfer materials after a rightful rejection. Licenses do not grant licensee a right to underlying data.	The sale of goods presumes no norm of confidentiality.
Delivery of Product	Intangibles may be "delivered" computer-to-computer without human contact.	The sale of goods is marked by a physical delivery of tangible goods. The buyer has the right to inspect goods. U.C.C. § 2-512.
Standard of Performance	Software is rarely, if ever, "bug-free." With the licensing of intangibles, substantial performance is the de facto performance standard.	Buyers of goods have a right to reject goods if they "fail in any respect to conform to the contract." U.C.C. § 2-601.
Remedies	Remedies may include remedies for breach of confidentiality or breach of the warranties against failure of system integration, or unauthorized access by third parties, viruses and extraneous data.	Sections 2-703 and 2-711 of Article 2 index the range of remedies with respect to the sale of goods.
Nature of Relationship	Mass-marketed licenses are one-shot transactions. Customized license agreements are generally relational and long-term. Vendors often customize, support or maintain software.	While one-shot transactions predominate the mass-market sale of goods, Article 2 covers long-term requirements or output contracts.

As Diagram One reveals, there is little overlap between the attributes of sale of tangibles and licensing of intangibles. The licensing of an Internet security product is based upon entirely different assumptions than is an Article 2 sale. While courts have attempted to stretch Article 2 to accommodate the licensing of intangibles, the principles of Article 2 do not correspond to the commercial reality of licensing transactions in most significant respects. For example, the performance obligations of a buyer under Article 2 are a poor match for the obligations of a licensee, as are warranties under Article 2.²⁹⁶ Article 2 remedies are also ill-equipped to address licensing transactions. There is uncertainty whether a software licensor has the right to include a disabling device in its program as the functional equivalent of self-help repossession. Article 2 allows a buyer to reject the whole product if it fails "in any respect to conform to the contract."²⁹⁷ Would this "perfect tender rule" of Article 2 permit a licensee to reject a program arbitrarily because it contains a few lines of errant code? The mass-marketing of some Internet security software applications most closely resembles the sale of goods, but even here there are significant differences. For example, goods under U.C.C. sales law are freely assignable, whereas licensors typically attempt to restrict assignability. This is far afield from an Article 2 sale.

There is a great deal of uncertainty as to how, or if, courts could reconcile U.C.C. sales principles with the licensing of Internet security products. Article 2 does not address such fundamental issues as the enforceability of shrink-wrap licensing, warranty disclaimers, third-party rights and appropriate remedies for the breach of a license agreement. Without clear rules, there will be uncertainty in the allocation of risk in Internet security contracts.

296. In the sale of goods, a buyer is expected to accept or reject goods promptly. However, a licensee may need more time to reject non-conforming software products. Many customized licenses provide for an "acceptance testing period." However, § 2-602(1) states that the rejection must be "within a reasonable time after their delivery or tender." U.C.C. § 2-602(1) (1990). Should a licensee be deemed to have a "reasonable opportunity" for acceptance testing? Section 2-602(1) provides only a "reasonable opportunity to inspect" the goods. *Id.* This doctrine seems inapplicable to complex computer contracts where acceptance testing may extend over a number of months. See *Beasley Ford, Inc. v. Burroughs Corp.*, 361 F. Supp. 325 (E.D. Pa. 1973), *aff'd*, 493 F.2d 1400 (3d Cir. 1974) (holding that eight months was not an unreasonably long time given the complexity of a computer).

Under Article 2 sales, no implied warranties are contemplated for "system integration," "confidentiality of data," or "data integrity." See U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995).

297. U.C.C. § 2-601 (1990).

IV. REGULATION OF INTERNET SECURITY PRODUCTS UNDER PROPOSED U.C.C. ARTICLE 2B

The importance of security software and other intangibles to the National Information Infrastructure and to our economy cannot be underestimated. The regulation of transactions involving intangibles, such as security software, requires a specialized body of law that balances the competing interests of consumers and stakeholders in the software industry. Current law has proven inadequate for this purpose. Article 2 does not even address the licensing of intangibles, which is not surprising since the U.C.C. was completed in 1951, decades before the rise of software, telecommunications services and multimedia entertainment services. Due to the inadequacies of existing law, forging a contract law for intangibles has become a top priority in the revision of the Uniform Commercial Code.²⁹⁸ The result is Article 2B, the proposed software licensing law. Article 2B has the potential to modernize the general licensing of intangibles like security software. Part IV of this article advocates the adoption of the proposed Article 2B as a comprehensive legal framework for regulating the licensing of security software and other transactions involving intangibles.

At the time of the writing of this article, a draft of Article 2B is not available for public review; it is, however, scheduled to be available in early 1996. The earliest that Article 2B will be approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) is the summer of 1996.²⁹⁹ NCCUSL appointed Raymond T. Nimmer to draft the new article.³⁰⁰ Professor Nimmer co-drafted Article 2B's ill-fated predecessor—the "hub and spoke" paradigm for Article 2.³⁰¹ Since it is likely that much of the law

298. See Amelia H. Boss, *Developments on the Fringe: Article 2 Revisions, Computer Contracting, and Suretyship*, 46 BUS. LAW. 1803 (1991); Jeffrey B. Ritter, *Software Transactions and Uniformity: Accommodating Codes Under the Code*, 46 BUS. LAW. 1825 (1991) (describing U.C.C. revision project to incorporate software into Article 2).

299. Future drafts of the software licensing article will be available from the Commission. The Commission's address and telephone number are: National Conference of Commissioners on Uniform State Laws, 676 North St. Clair Street, Suite 1700, Chicago, IL 60611; (312) 915-0195. Copies of the Sept. 10, 1994 discussion draft are available from Chicago-Kent Law School's site on the World Wide Web, "<http://www.kentlaw.edu/ulc/>."

300. Thom Weidlich, *Commission Plans New U.C.C. Article*, NAT'L L. J., Aug. 28, 1995, at B1. Raymond Nimmer, a professor of law at the University of Houston, is a well-known legal academic and computer law practitioner. See Raymond T. Nimmer, *Intangibles Contracts: Thoughts of Hubs, Spokes, and Reinvigorating Article 2*, 35 WM. & MARY L. REV. 1337 (1994).

301. In March of 1995, NCCUSL approved a "hub and spoke" paradigm for the reconstruction of Article 2. The "hub and spoke" arrangement assumed that all

developed in the "hub and spoke" will be tracked quite closely in Article 2B,³⁰² this article uses the "hub and spoke" draft as a prototype for discussing the new software licensing law.

Article 2 transactions share general principles of law such as contract formation, unconscionability and the statute of frauds. See UNIFORM COMMERCIAL CODE: REVISED ARTICLE 2, (Proposed "Hub and Spoke" Draft, Feb. 10, 1995) (Raymond Nimmer, Reporter). The "hub" of Article 2 consisted of the general principles which were to apply to discrete chapters or "spokes" of Article 2, such as sales, leases or licenses.

The "hub and spoke" model was opposed from the beginning by software stakeholders. Drafts of the "hub and spoke" licensing chapter were circulated to diverse groups including the Software Publishers' Association, Business Software Alliance, Information Industry Association, Software Coalition, AIPLA, ABA Business Law Section, ABA Section on Intellectual Property, ABA Section of Science and Technology, Licensing Executives Society, Computer Law Association and local Bar associations. See generally Corinne Cooper, *The Madonnas Play Tug of War with the Whores or Who Is Saving the U.C.C.?*, 26 LOY. L.A. L. REV. 563 (1993) (arguing that the U.C.C. revision process must be vigilant and must not be captured by special interest groups); Edward L. Rubin, *Thinking Like a Lawyer, Acting Like a Lobbyist: Some Notes on the Process of Revising U.C.C. Articles 3 and 4*, 26 LOY. L.A. L. REV. 743 (1993) (describing the interest group politics of U.C.C. revision).

The Software Publishers Association (SPA) expressed early opposition to the "hub and spoke" paradigm. The SPA claimed that "[e]xcept for [two people], no one on the 16-member drafting committee working on Article 2 of the U.C.C. seems to have any experience in licensing, high-technology matters, and intellectual property." Groner, *supra* note 288, at 1. The SPA also criticized the draft as being skewed in favor of the consumer. *Id.* An in-house attorney for a Fortune 500 firm contended that the Article 2 drafters are "pro-buyer" and "anti-seller." *Id.* (quoting Norman Rosen, Counsel to General Electric). Norman Rosen attributed much of the pro-consumer bias to the composition of the drafting committee: "Many of the law professors on the panel have a pro-consumer bias, or are liberals." *Id.*

The "hub and spoke" paradigm was also critiqued "by several representatives of the software industry and Bar, and by some commercial law scholars." Thomas J. McCarthy, Corporate Counsel, DuPont Legal, Chair of the ABA Business Law Section Task Force on the Revision of Article 2, *NCCUSL Article 2 Drafting Committee: October 14-16, 1994 Meeting*, Oct. 21, 1994, at 1. The Computer Law Committee of the Association of the Bar of the City of New York concluded that the Draft should consider "eliminating the 'hub and spoke' structure." Letter from Ronald Abramson, Committee Chair, The Association of the Bar of the City of New York, Committee on Computer Law, to National Conference of Commissioners on Uniform State Laws 7 (Oct. 7, 1994) (on file with author). Some argued that intangible licensing has little in common with the "sale of goods." Zan Hale, *U.C.C. Article 2 Drafting Committee Faces Critics*, CORP. LEGAL TIMES, Oct. 1994, at 24.

The death knell of the "hub and spoke" paradigm was sounded in August of 1995 when NCCUSL abandoned the model of a "hub and spoke" in favor of a stand-alone software article [hereinafter proposed Article 2B]. See generally Weidlich, *supra* note 300, at B1 (reporting that NCCUSL rejected the restructuring of the U.C.C. in the "hub and spoke"). Many of the legal doctrines for resolving software issues developed in the "hub and spoke" will be reformulated in the separate software article.

302. We do not suggest that there is as yet an engineered consensus on controversial issues such as the content of performance warranties, remedies, or the enforceability of shrink-wrap licenses. New Article 2B, like its predecessor, will also be revised by the U.C.C. revision process. However, the fact that Raymond Nimmer, drafter of the

In addition to Professor Nimmer (Article 2B's "Technology Reporter"), the key players in the formation of Article 2B are: the American Bar Association (ABA),³⁰³ the NCCUSL³⁰⁴ and the American Law Institute (ALI).³⁰⁵ However, what should or should not be incorporated within the scope of Article 2B is a subject of much debate. For example, lawyers representing large commercial buyers of network systems favor remedies which provide them with assurance that consequential damages will be recouped. If a vendor of an Internet security product represents that its product insures "bullet-proof security" and that system fails due to the licensor's fault, the licensee will want to recover consequential damages.³⁰⁶

licensing chapter of the "hub and spoke," was reappointed to draft the separate article provides a strong indication Article 2B will share much common ground with the abandoned "hub and spoke."

303. The Software Contracting Subcommittee of the Uniform Commercial Code Committee of the Business Law Section of the American Bar Association has been a key player in the drafting of the software licensing provisions. The Subcommittee is chaired by Donald A. Cohn, Senior Counsel of DuPont, and Ellen Kirsh, Vice President and General Counsel of America Online. The Subcommittee is composed of corporate counsel, experienced software lawyers, computer law practitioners, legal academics and consumer representatives. The Subcommittee has engaged in a number of projects. One of the tasks has been to analyze and provide comments to the NCCUSL about the issuance of the "hub and spoke" draft. The Subcommittee's work reflects an ABA position on the proposed draft. The Subcommittee also coordinates with other ABA sections such as Intellectual Property and Law and Technology. The Subcommittee provides the Technology Reporter with issue papers.

Since 1992, the Subcommittee has also been divided into working groups. Michael Rustad, co-author of this article, has been a Task Leader for third-party and scope issues and was appointed Co-Chair of the Task Force on General Provisions of the Proposed U.C.C. Article 2B on the licensing of intangibles in September of 1995.

304. Along with the American Law Institute, the NCCUSL approves proposed drafts and votes on whether to submit a completed draft to state legislatures. NCCUSL appointed the Technology Reporter and the drafters of revised Article 2.

305. The American Law Institute of Philadelphia, Pennsylvania is a key sponsoring organization for the Code. Stephen C. Veltri & Ronald S. Gross, *Introduction to the Uniform Commercial Code Survey: The Role of the Courts in a Time of Change*, 49 BUS. LAW. 1827, 1830 (1994). The ALI was the promulgator of the influential Restatements and most other successful codification projects. Its membership is composed of distinguished practitioners, judges and legal academics. Dom Calabrese et al., *Karl Llewellyn's Letters to Emma Cortsvet Llewellyn from the Fall 1941 Meeting of the National Conference of Commissioners on Uniform State Laws*, 27 CONN. L. REV. 523, 525 (1995).

306. Consequential damages are recoverable under § 2-715(2) of current Article 2. Recovery of consequential damages provides recovery for losses beyond the basic damages recovery found in § 2-714. The failure of Internet security may result in realized losses, economic loss, or even personal injury. An attorney for Consumers Union believes that software contracts should offer the same protection as do contracts in the sale of goods: "Customers expect the product to work. When you open the box, it's just like a toaster. If that's not the business you're in, you'd better make it clear." Groner, *supra* note 288, at 26.

In order to learn more about what practitioners would like incorporated within the scope of Article 2B, co-author Michael Rustad surveyed the membership of the Computer Law Association (CLA Survey).³⁰⁷ The CLA Survey's goal was to collect data on the extant and emergent software licensing law by querying lawyers who work in this field.³⁰⁸ The quantitative findings of the CLA Survey are reproduced in Appendix B. Some of the results are also described in the text to give the reader an idea of practitioners' concerns.³⁰⁹

This part is divided into two subparts. Subpart IV.A. discusses each section of the proposed Article 2B—in order to appreciate the effective, coherent legal regime afforded by Article 2B, it is necessary to first understand its basic provisions—and discusses Article 2B's effect on mass-market licenses. Subpart IV.B. presents our case for adopting Article 2B for regulating transactions involving Internet and network security software.

307. This empirical study was conducted in the Fall of 1994. The Computer Law Association (CLA) membership consists of intellectual property lawyers who develop, distribute and use computer technology. We designed a national survey on the computer law practitioner's view of software licensing issues as well as the proposed licensing chapter of Article 2 of the U.C.C. The instrument was field tested in the Summer of 1993. This survey was mailed to all 950 North American members of the CLA in August of 1994.

We received 147 responses to the survey which represented a 15% response rate. Members of the CLA responding to our survey represented an excellent cross-section of lawyers working with software law. Respondents were from 29 states, the District of Columbia and Canada. The majority of respondents were from Massachusetts, California, the District of Columbia, Virginia and New York. The respondents were 86% male and 14% female. The sample reflected a reasonable balance between attorneys who represented vendors and buyers. The vast majority of these computer lawyers had five or more years of software legal experience. Our sample included representatives of diverse branches of the software industry, including on-line providers as well as large-scale users from the general corporate community. In the CLA Survey's second section, respondents were asked to state their agreement with statements concerning various aspects of software law. Topics surveyed were the definition of mass-marketed software, assignability, warranty, disclaimers, shrink-wrap licenses and scope of rights. The third section presented five software legal hypotheticals and asked how licensing law should resolve the issues raised by each scenario. The final section surveyed respondents' awareness and attitude toward the software "spoke" of proposed revisions to Article 2 of the U.C.C. See Michael Rustad et al., *An Empirical Analysis of Software Licensing Law and Practices (Part Two)*, 10 (4) COMPUTER L. ASS'N BULL. 3 (1995).

308. *Id.*

309. Throughout this part, we cite to specific comments of some CLA respondents. Anecdotal comments made by respondents were assured the same privacy and confidentiality as their completed CLA surveys. All surveys, including respondents' unstructured comments as quoted within this article, are on file with co-author Michael Rustad.

A. Anatomy of Proposed U.C.C. Article 2B

The proposed Article 2B will likely consist of six parts: (1) General Provisions; (2) Formation and Construction; (3) Performance and Construction; (4) Warranties; (5) Effect of License on Third Parties; and (6) Default and Remedies.³¹⁰ We will discuss each part in turn, detailing the likely provisions and providing practitioners' perspectives on each topic based on the results of the CLA Survey. We will also discuss the controversy surrounding Article 2B's treatment of mass-market licenses.

1. GENERAL PROVISIONS

The general provisions section of Article 2B will likely contain definitions previously located in both the "hub" and "spoke" provisions for intangibles.³¹¹ The proposed licensing article will reconcile the "hub" and "spoke" sections in a stand-alone article which will include terminology applicable to the licensing of security software. The proposed Article 2B will apply to "intangible contracts and agreements incidental to intangible contracts"³¹² and will encompass concepts such as the mass-market license,³¹³ "intangible,"³¹⁴ "consumer contracts,"³¹⁵ "record,"³¹⁶ and "signed."³¹⁷ Similarly, the new software licensing article will quite likely validate electronic contract formation by exchange of records.³¹⁸

One of the key general provisions will be the definition of "intangibles." As in the "hub and spoke" draft, intangibles will be defined as "data, information, software and any intellectual property rights associated with the data, information, or software, whether or not the intangible is embodied in tangible form."³¹⁹ The provisions

310. These six parts correspond to the main elements of the "hub and spoke" paradigm.

311. The General Provisions of the "hub and spoke" draft covered definitions, scope, choice of law and transfer of rights provisions. U.C.C., Rev. Article 2 (Proposed "Hub and Spoke" Draft, Feb. 10, 1995) (Raymond Nimmer, Reporter).

312. U.C.C. § 2-102(a) (Proposed Draft, Feb. 10, 1995). Under the proposed Article 2B, the following will specifically be *excluded* from U.C.C. treatment: 1) patents; 2) trade secrets; 3) know-how or similar intangibles unrelated to software or a computer program; and 4) embedded software (*e.g.*, PROM in a pickup truck). *See, e.g.*, U.C.C. § 2-2102(C) (Proposed Draft, Feb. 10, 1995).

313. *See, e.g.*, U.C.C. § 2-2101(1) (Proposed Draft, Feb. 10, 1995).

314. *See, e.g.*, U.C.C. § 2-102(a)(27) (Proposed Draft, Feb. 10, 1995).

315. *See, e.g.*, U.C.C. § 2-102(a)(12) (Proposed Draft, Feb. 10, 1995).

316. *See, e.g.*, U.C.C. § 2-102(a)(39) (Proposed Draft, Feb. 10, 1995).

317. *See, e.g.*, U.C.C. § 2-102(a)(42) (Proposed Draft, Feb. 10, 1995).

318. *See, e.g.*, U.C.C. § 2-102(a)(22) (Proposed Draft, Feb. 10, 1995).

319. U.C.C. § 2-102(a)(27) (Proposed Draft, Feb. 10, 1995).

will probably also use a definition of an "intangible contract" similar to that used in the "hub and spoke" version: "a license, software contract, continuous access contract or other agreement to transfer rights in intangibles."³²⁰ Thus, the licensing of security software, such as an anti-virus program, would qualify as an "intangible contract." The proposed Article will probably incorporate the "hub and spoke" definition of "computer program": "a set of statements or instructions" that is "capable of causing a machine having information processing capabilities to indicate, display, perform or achieve a function or result."³²¹ Security software fits this definition.³²² Furthermore, the licensing of security software is a method of transferring rights that will be validated by the proposed general provisions.³²³ The proposed Article 2B's definitions will provide the appropriate legal infrastructure for approaching and managing the licensing of security software.

2. FORMATION AND CONSTRUCTION

The hallmark of Article 2 contract formation, which the proposed Article 2B will likely incorporate, is its flexibility and realism. Article 2's section 2-204, for example, is a liberal formation rule, requiring only that formation be "sufficient to show agreement."³²⁴ The U.C.C. permits a contract for sale of goods to be formed even though one or more of its terms are left open, as long as a reasonably certain basis exists for a court to grant an appropriate remedy in the event of breach.³²⁵ Like Article 2's default terms for sales transactions,³²⁶ the proposed Article 2B will likely provide

320. U.C.C. § 2-102(a)(28) (Proposed Draft, Feb. 10, 1995).

321. U.C.C. § 2-102(a)(8) (Proposed Draft, Feb. 10, 1995).

322. Security software is essentially a set of instructions that causes a computer to achieve the function of excluding intruders or protecting confidentiality. Security is the task or result of the software program. Thus, the intangible instructions of security software will be easily accommodated in Article 2B.

323. The "hub and spoke" draft defined the "license" as "an agreement for a transfer of rights in an intangible where the rights transferred are conditional or limited, whether or not the agreement provides for delivery of tangible property that contains the intangible. The term does not include the reservation or creation of a security interest in an intangible." U.C.C. § 2-102(30) (Proposed Draft, Feb. 10, 1995).

324. U.C.C. § 2-204(1) (1990).

325. U.C.C. § 2-204(3) (1990). Additionally, section 2-206 supplements sections 2-204 and 2-205 in setting forth how a contract is formed under Article 2. Section 2-206(1)(b), for example, provides that an "order for prompt shipment . . . invites acceptance by a prompt promise to ship or by prompt shipment." U.C.C. § 2-206(1)(b) (1990).

326. See U.C.C. §§ 2-305 to -311 (1990) (affixing default provisions relating to price, output and requirement contracts; method, place and time of delivery; time and method of payment; and assortment of goods).

default, general obligation gap-fillers appropriate to the licensing of intangibles.

The presumption of confidentiality, for example, would be a gap-filler where the intangible contract is silent.³²⁷ Other key gap-fillers in the proposed Article 2B will include scope of the license, number of users, number of machines, scope of the grant of the license and time of license creation.³²⁸ In addition, licensees will not be automatically entitled to developments or modifications of software in the absence of agreement,³²⁹ nor will they be deemed to have a right to an intangible's underlying data or source code³³⁰ unless the license expressly grants that right.³³¹ Article 2B will likely also define default rules for location and use restrictions. In the absence of agreement to the contrary, a licensee of Internet security software will be able to use the product in any location that is reasonable.³³² If a licensee exceeds the scope of use restrictions, it will be in breach.³³³ Thus, the proposed Article 2B's gap-filler provisions will directly

327. *See, e.g.*, U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

328. The proposed Article 2B will probably provide the gap-filler that a license is non-exclusive, meaning that a licensee will only have the right to use a single copy of the software at a single time, on a single machine. *See, e.g.*, U.C.C. § 2-2204(a) (Proposed Draft, Feb. 10, 1995). Of course, the parties will be free to negotiate around these provisions. Another Article 2B gap-filler will be the definition of "all rights" or "all uses" of a license to cover all future uses. *See, e.g.*, U.C.C. § 2-2204(b)(1) (Proposed Draft, Feb. 10, 1995). Similarly, the proposed Article will likely cover all rights necessary to use rights transferred by the license agreement. *See, e.g.*, U.C.C. § 2-2204(b)(2) (Proposed Draft, Feb. 10, 1995).

329. *See, e.g.*, U.C.C. § 2-2205 (Proposed Draft, Feb. 10, 1995). However, if a vendor does grant its customer software enhancements, the contract term will likely be defined by reasonableness and industry standards. *Id.*

330. Many software licensing contracts specify that only object code will be supplied to the licensee and that the source code will remain with the licensor. This is because the distribution of the source code may jeopardize its status as a trade secret. A computer program is generally written in an easily understood programming language. This is referred to as "source code." This source code must be translated into corresponding machine-readable instructions. The resulting set of instructions is referred to as "object code" and is, as a practical matter, unintelligible to anything but the machine for which it is designed. The source code and object code are treated as one for copyright purposes. "Because the object code is the encryption of the copyrighted source code, the two are to be treated as one work; therefore copyright of the source code protects the object code as well." *GCA v. Chance*, 217 U.S.P.Q. (BNA) 718 (1982).

331. *See, e.g.*, U.C.C. § 2-2206 (Proposed Draft, Feb. 10, 1995). As a result of this gap-filler, an on-line security provider, such as America Online, would not have to hand over the underlying data on its system unless this access was specified in the contract.

332. *See, e.g.*, U.C.C. § 2-2208 (Proposed Draft, Feb. 10, 1995).

333. *Id.* A breach would also occur if the licensee exceeded the designated number of copies of a software program. *See id.*

respond to the realities of Internet security software licensing transactions.

3. PERFORMANCE AND CONSTRUCTION

The proposed Article 2B's "Performance and Construction" part will likely include tender, acceptance, rejection and revocation provisions. The net effect of these provisions will be to provide a framework of general construction and performance principles which accord with the commercial reality of licensing intangibles transactions, and thus security software transactions. Each provision will be discussed in turn.

a. Tender and Acceptance

Under Article 2, the delivery of goods triggers the buyer's duty "to accept and pay in accordance with the contract."³³⁴ The proposed Article 2B will likely replace the concept of "delivery" with that of "transfer of rights." A transfer of rights will consist of the "grant of a right to have access to, modify, disclose, distribute, copy, use, have used on behalf of the transferee, or otherwise take action with respect to an intangible coupled with any actions necessary to enable the transferee to exercise those rights."³³⁵ Under the proposed Article 2B, the licensor's tender will thus occur upon the transfer of rights to the intangibles,³³⁶ by either physical delivery or electronic means.³³⁷ Similarly, the licensee's tender of payment may be made through physical, electronic or any other reasonable means.³³⁸

With respect to tender, Article 2 employs the "perfect tender rule," affording an aggrieved buyer the option to reject goods "if the goods or the tender of delivery fail in any respect to conform to the contract."³³⁹ However, this logic fails in the context of security software licensing because "minor flaws ('bugs') are common in virtually all software."³⁴⁰ Under a perfect tender rule licensees would be able to routinely reject the "flawed" software since it would probably not conform to the licensing agreement. To correct this, the

334. U.C.C. § 2-301 (1990).

335. U.C.C. § 2-102(a)(51) (Proposed Draft, Feb. 10, 1995).

336. *See, e.g.*, U.C.C. § 2-2104 (Proposed Draft, Feb. 10, 1995).

337. *See, e.g.*, U.C.C. §§ 2-2301, 2-2302 (Proposed Draft, Feb. 10, 1995).

338. *See, e.g.*, U.C.C. § 2-2303(b) (Proposed Draft, Feb. 10, 1995).

339. U.C.C. § 2-601 (1990).

340. U.C.C. § 2-2106 cmt. 6 (Proposed Draft, Sept. 10, 1994).

proposed Article 2B will likely replace the perfect tender rule with a "substantial performance" standard.³⁴¹

The relational or ongoing nature of software licensing contracts lends additional support for a substantial performance standard. Some security software has a period of "acceptance testing" in which minor bugs are fixed. Other transactions involve a maintenance contract or provide updates as a program is improved. Unstructured interviews conducted as part of the CLA Survey revealed that most attorneys favor the substantial performance standard rather than the perfect tender rule.³⁴²

b. Rejection and Revocation

As with Article 2, a software licensee under the proposed Article 2B will likely have a flexible array of options upon the licensor's improper tender, including rejection³⁴³ and revocation.³⁴⁴ These provisions are discussed more fully in part 6, in the context of defaults and remedies.

4. WARRANTIES

The legal structure for security software must resolve the issues of express and implied warranties and the clauses that attempt to limit damages. The proposed Article 2B's warranty provisions will probably closely fit the realities of security software. The CLA Survey indicated that the lack of uniform warranty standards for software licensing constituted one of the primary arguments for codification.³⁴⁵ One attorney wrote, "Throughout the country, these

341. See, e.g., U.C.C. § 2-2306 (Proposed Draft, Feb. 10 1995). The substantial performance standard does not mean, however, that minor flaws will be tolerated. Dean Nimmer states:

A substantial performance rule does *not* hold that substantial (but imperfect) performance of a contract is not a breach. To the contrary, both the common law and the rule here treat substantial (but imperfect) performance as a breach of contract. The significance of the concept of substantial performance lies in the remedy available to the injured party. Unless a breach is material, it cannot be used as an excuse to void or avoid the contract obligation. A licensee who receives substantial (but imperfect) performance from the licensor, cannot reject the initial tender or cancel the contract on that account, but it can obtain financial satisfaction for the less than complete performance.

U.C.C., Rev. Article 2, Sales, Chapter 3: Licenses, Prefatory Note 9 (Proposed Draft, Sept. 10, 1994) (Raymond Nimmer, Reporter).

342. CLA Survey, *supra* note 307.

343. See, e.g., U.C.C. § 2-2306(a) (Proposed Draft, Feb. 10, 1995).

344. See, e.g., U.C.C. § 2-2311 (Proposed Draft, Feb. 10, 1995).

345. CLA Survey, *supra* note 307.

are resolved differently depending on the jurisdiction. Uniform rules would be extremely helpful in this area."³⁴⁶ This part will discuss how the proposed Article 2B will likely address both express and implied warranties, as well as disclaimers and limitations of such warranties.

a. Express Warranties

The proposed Article 2B's express warranty provisions for software licensing will probably be substantially similar to those presently provided for the sale of goods under Article 2.³⁴⁷ For example, affirmations of fact which form part of the "basis of the bargain" will likely become part of the agreement between the parties at the time of initial transfer of rights.³⁴⁸ However, if mass-marketed information or data is the subject of the transfer, there will likely be no warranty of accuracy in the information without an express warranty to a specific licensee.³⁴⁹ A developer of pre-packaged software who gives written warranties to consumers will not only be subject to the provisions of the proposed Article 2B, but will also likely be subject to the federal Magnuson-Moss Act.³⁵⁰

346. *Id.*

347. The methodology for creating express warranties for software licensing is substantially similar to the law of sales. A licensor of security software could create express warranties through samples, models, demonstrations or descriptions. Words such as "warranty" or "guaranty" will be unnecessary. The sole test of an express warranty in a software licensing transaction will be whether the statement constitutes part of the basis of the bargain. Compare U.C.C. § 2-2402 (Proposed Draft, Feb. 10, 1995) with U.C.C. § 2-313 (1990). See, e.g., *infra* App. A § 14.

348. See, e.g., U.C.C. § 2-2402(a)(1) (Proposed Draft, Feb. 10, 1995).

349. See, e.g., U.C.C. § 2-2402(c) (Proposed Draft, Feb. 10, 1995).

350. The Magnuson-Moss Warranty—Federal Trade Commission Improvement Act provides remedies for consumers against all warrantors of products. 15 U.S.C. § 2301, 88 Stat. 2183 (1975). It defines a consumer as follows:

The term "consumer" means a buyer (other than for purposes of resale) of any consumer product, any person to whom such product is transferred during the duration of an implied or written warranty (or service contract) applicable to the product, and any other person who is entitled by the terms of such warranty (or service contract) or under applicable State law to enforce against the warrantor (or service contractor) the obligation of the warranty (or service contract).

15 U.S.C. § 2301(3) (1975).

Suppliers are subject to Magnuson-Moss warranties. A "supplier" is any person selling consumer products. 15 U.S.C. § 2301(4) (1975). A "warrantor" is any supplier who gives a written warranty or who is obligated under an implied warranty. 15 U.S.C. § 2301(5) (1975). The Magnuson-Moss Warranty Act provides rules for two types of written warranties, full and limited. Full warranties are described in 15 U.S.C. § 2304 (1975). A full warrantor must give a consumer a full refund or replacement without charge after a product fails and after a reasonable number of

b. Implied Warranties

Implied warranties for software licensed under the proposed Article 2B will likely be quite different than implied warranties for goods under Article 2. Nevertheless, Article 2's implied warranty of "merchantability"³⁵¹ and implied warranty of "fitness for a particular purpose"³⁵² will likely have their functional equivalents in the proposed Article 2B. These will be the implied warranty of quality³⁵³ and the implied warranty of system integration,³⁵⁴ respectively. The proposed Article will probably create two other implied warranties, an electronic security warranty³⁵⁵ and an implied warranty for information and services.³⁵⁶ The implied warranties for electronic security and system integration will be specifically tailored to the licensing of intangibles. The implied warranty for system integration³⁵⁷ would apply where the licensee relies upon the licensor's expertise to make the software suitable for the licensee's purposes. When the licensee's reliance is disclosed by the contract, or from other circumstances, the licensor will likely be subject to an implied warranty of "reasonable care" and "workmanlike effort" to achieve the licensee's purposes.³⁵⁸ Moreover, if the product is an integrated system, the licensor will likely be further subject to the

attempts at repair. Consumers may obtain damages, legal, or equitable relief under the act. *See* 15 U.S.C. § 2310(d) (1975).

Assuming that security software is sold to a consumer and "written warranties" are given, Magnuson-Moss would likely apply. A consumer damaged by the failure of Internet security software may bring suit "for damages and other legal and equitable relief." 15 U.S.C. § 2310(d)(1) (1975). The Magnuson-Moss Warranty Act would permit a dissatisfied licensee to recover attorney's fees "as part of the judgment." 15 U.S.C. § 2310(d)(2) (1975). Assuming Magnuson-Moss applied to mass-marketed security software, the Federal Trade Commission (FTC) rules for warranties would also apply. 40 Fed. Reg. 60188 (1975) (codified at 16 C.F.R. § 701) The FTC rules also provide for informal dispute settlement. 40 Fed. Reg. 60215 (1975) (codified at 16 C.F.R. § 703).

351. *See* U.C.C. § 2-316 (1990).

352. U.C.C. § 2-315 (1990).

353. *See, e.g.*, U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995). Non-data items of a transaction, such as protective "boot disks" for laptop computers, will be subject to the implied warranty standard of "substantial conformance." *See, e.g.*, U.C.C. § 2-2403(a) (Proposed Draft, Feb. 10, 1995).

354. *See, e.g.*, U.C.C. § 2-2405(c) (Proposed Draft, Feb. 10, 1995).

355. *See, e.g.*, U.C.C. § 2-2406 (Proposed Draft, Feb. 10, 1995).

356. *See, e.g.*, U.C.C. § 2-2404 (Proposed Draft, Feb. 10, 1995). Information and services components of a software licensing transaction will be governed by the implied warranty standard of "reasonableness and workmanlike effort." *See, e.g.*, U.C.C. § 2-2404(a) (Proposed Draft, Feb. 10, 1995).

357. *See, e.g.*, U.C.C. § 2-2405 (Proposed Draft, Feb. 10, 1995).

358. *See, e.g.*, U.C.C. §§ 2-2405(a), (b) (Proposed Draft, Feb. 10, 1995).

implied warranty that its components "will function together as a system substantially consistent with the goals of the licensee."³⁵⁹

The implied warranty for electronic security will be applicable to the transfer of rights by electronic access.³⁶⁰ This implied warranty will require the licensor *and* the licensee to use reasonable care to exclude: 1) unauthorized access by third parties; 2) undisclosed programs; and 3) extraneous data.³⁶¹ The standard will probably be the same as that used in the "hub and spoke" version—whether the allowance or inclusion of the above could "reasonably be expected to damage data, software systems, or operations."³⁶²

c. Disclaimers and Limitations

Under Article 2, a disclaimer occurs when a seller of goods uses language or conduct to negate or limit implied warranties.³⁶³ Disclaiming warranties under the proposed Article 2B will likely parallel Article 2's provisions with two notable exceptions: 1) the "writing" requirement for modification or exclusion of warranties may expressly be met by means of an electronic record;³⁶⁴ and 2) any exclusion with regard to a *consumer* will be *inoperative* unless the consumer "expressly" consents.³⁶⁵ However, while reasonable disclaimers will likely be permitted,³⁶⁶ unconscionable disclaimers will not be enforced, nor will remedies that fail of their essential purpose.³⁶⁷

In the CLA Survey, computer lawyer respondents were asked for their opinion on how to resolve warranty issues for the licensing of intangibles. The extent to which the proposed Article 2B should permit vendors to disclaim or limit liability was a subject of great controversy in the CLA Survey. Article 2 already permits vendors to disclaim implied warranties by conspicuous use of terms such as "with all faults" or "as is."³⁶⁸ One respondent representing a large-scale

359. U.C.C. § 2-2405(c) (Proposed Draft, Feb. 10, 1995).

360. *See, e.g.*, U.C.C. § 2-2406 (Proposed Draft, Feb. 10, 1995).

361. *See id.*

362. *Id.*

363. *See* U.C.C. § 2-316 (1990). For an example of such a disclaimer, *see* App. A § 14, *infra*.

364. *See, e.g.*, U.C.C. § 2-2407(b) (Proposed Draft, Feb. 10, 1995).

365. *Id.*

366. *See, e.g.*, U.C.C. § 2-2407 (Proposed Draft, Feb. 10, 1995).

367. *See, e.g.*, *Riley v. Ford Motor Co.*, 442 F.2d 670 (5th Cir. 1971) (exclusive remedy failed of its essential purpose when repeated car repair attempts were ineffective). *See also* *RRX Indus., Inc. v. Lab-Con, Inc.*, 772 F.2d 543, 547 (9th Cir. 1985) (holding that a disclaimer of consequential damages was unenforceable).

368. U.C.C. § 2-316(3)(a) (1990).

vendor argued that the law of software licensing "should permit a software vendor to contractually limit the end-user's remedy for breach of warranty to repair, replacement or refund."³⁶⁹ An attorney with a corporate law firm thought it important to clarify the extent that lost profits and consequential damages could be disclaimed.³⁷⁰ These issues arise in virtually every software performance dispute and Article 2B will likely provide a guide for resolving such issues.³⁷¹

5. EFFECT OF LICENSES ON THIRD PARTIES

a. Transfer of Title of Tangibles and Intangibles

Under Article 2, a buyer obtains title to the good, and power to transfer that title, when she pays the agreed price for the good.³⁷² In the software licensing context, a licensee obtains title to a copy of the intangible and may use that copy in any manner consistent with the licensing agreement.³⁷³ The proposed Article 2B will likely make clear that transfer of title to the copy (i.e., a copy of the software code) does not transfer title to the intangible (i.e., the software code), and therefore the licensee does not have power to transfer title to the intangible itself, unless this is explicitly agreed to and stated in the licensing agreement.³⁷⁴ Thus, the proposed Article 2B will essentially provide that a security software licensing agreement will determine the licensee's rights to transfer rights to a third party.³⁷⁵

b. Assignment of Licenses

The law of assignment must also be adjusted to accommodate the licensing of security software. The proposed Article 2B will likely codify the general rule that a licensee generally may not assign or

369. CLA Survey, *supra* note 307.

370. *Id.*

371. In general, the proposed Article 2B will probably treat licensing arrangements resembling the sale of goods as having product-quality warranties. *See, e.g.*, U.C.C. § 2-2403 (Proposed Draft, Feb. 10, 1995). In contrast, a lesser warranty will likely be given for process-oriented transactions. *See, e.g.*, U.C.C. § 2-2404 (Proposed Draft, Feb. 10, 1995). This bifurcated warranty protection follows case law on sales and services. Warranties are generally provided for in sales, but not services. For a superb discussion of warranty issues in the proposed Article 2B, see Feldman, *New Draft, supra* note 264. *See also* Feldman, *Warranties, supra* note 274.

372. *See* U.C.C. § 2-301 (1990).

373. *See, e.g.*, U.C.C. § 2-2501 (Proposed Draft, Feb. 10, 1995); *infra* App. A § 6.

374. *See, e.g.*, U.C.C. § 2-2501 (Proposed Draft, Feb. 10, 1995); *infra* App. A § 13(b).

375. *Id.*

otherwise transfer a nonexclusive license.³⁷⁶ It will also provide that a licensor may freely assign his rights, provided the licensee's duties are not materially changed and the licensee's trade secrets and confidential information are not disclosed.³⁷⁷ In certain circumstances, a licensee will be able to assign her rights. A licensee may assign her rights in a license if "the license was a mass-market license, the licensee owned the copy of the intangibles, and the licensee transfers ownership of that copy and all other copies made by it pursuant to the license or applicable intellectual property law to its transferee."³⁷⁸

Many CLA Survey participants perceived assignability issues as a high priority for resolution in the proposed Article 2B.³⁷⁹ Data from the CLA Survey on third-party issues reveals industry consensus on an end-user's right to assign or resell software, irrespective of any shrink-wrap or other restrictions on assignment. Specifically, 83% of the computer lawyers surveyed agreed that "the law should allow the end-user to assign or resell software."³⁸⁰ A corporate counsel's

376. U.C.C. § 2-2502(a) (Proposed Draft, Feb. 10, 1995). This prohibition against assignment is at odds with many other U.C.C. articles that favor free assignability. See Edwin E. Smith, *Article 9 in Revision: A Proposal for Permitting Security Interests in Nonassignable Contracts and Permits*, 28 LOY. L.A. L. REV. 335, 338 (1994) (citing U.C.C. §§ 9-318(4), 2-210(2) and 2A-303 as examples of the free assignability norm). See, e.g., *infra* App. A § 20(f).

377. See, e.g., U.C.C. § 2-2502(b) (Proposed Draft, Feb. 10, 1995). This proposed section grants the licensor a right to assign rights under a license. However, if the assignment results in a hardship to the licensee, the licensor's transfer to the third party is prohibited. *Id.*

378. U.C.C. § 2-2502(a)(4) (Proposed Draft, Feb. 10, 1995). This provision comports with commercial realities since much security software resembles goods when it is mass-marketed and distributed over the Internet as "shareware" or "freeware." In such circumstances, consumers believe they "own" the software, and with ownership they expect that they are free to transfer ownership of the software, in the same sense as if the software was considered a good. Therefore, any contractual restrictions on such software are essentially inconsistent with the expectations of consumers (i.e., that they "own" the software).

379. The CLA Survey did not address issues involving the unauthorized transfer of copies of computer programs as copyright infringements. Software licenses generally allow the licensee to use the software for its own internal information processing. However, most licenses do not permit third parties to make "copies." Section 117 of the Copyright Act permits the "owner" of a copy of a computer program to make or authorize the making of another copy as an "essential step" in the use of the program or for "archival purposes." 17 U.S.C. § 117 (1994). Vendors usually argue that licensees who make other copies are infringing the licensor's copyright.

380. CLA Survey, *supra* note 307. However, most of the CLA respondents would place some limitation on the assignability of licenses. CLA Survey, *infra* App. B question 2. Most respondents agreed that an end user should have the right to move the physical location of software. Sixty-three percent agreed that a user should have the right to assign or resell software, irrespective of any shrink-wrap restrictions. Another 63% agreed that a licensee should have the right to assign software to an

view on assignment was typical of most responding intellectual property attorneys: "As long as the scope of use is not expanded by an assignment, the vendor should have little objection about assigning software. [The] licensor should have no objection about an outsourcer using software on behalf of "Company X" so long as scope of use is not altered."³⁸¹ The proposed Article 2B's provisions could go a long way toward resolving the difficult problems of assignability.

c. Copying, Use and Location Restrictions

Article 2B will probably follow its "hub and spoke" predecessor in providing that, if a software contract license grants the right to use a single or specified number of copies of the software,³⁸² the licensee's "making or retaining additional copies or permitting simultaneous use by multiple users" will be considered a breach, unless otherwise permitted by copyright law.³⁸³ Furthermore, if the licensor does not specify location limits, software may be used in any reasonable location.³⁸⁴ A majority of the CLA Survey respondents support these use and location restrictions.³⁸⁵

6. DEFAULT AND REMEDIES

The remedies for licensors and licensees under the proposed Article 2B will likely differ from Article 2 remedies currently available to sellers and buyers. For example, licensors will likely have a right to recover consequential damages under the proposed Article 2B,³⁸⁶ a remedy not accorded aggrieved sellers under Article 2.³⁸⁷ The remedies for licensors and licensees will be discussed in turn.

outsourcer (a firm hired to manage data processing activities). For mass-marketed software licenses, most respondents believed that software law should reflect the norm of free assignability.

381. CLA Survey, *supra* note 307.

382. Many software licenses specify the number of copies of a program that may be used at the same time or at a given site. The draft does not currently address the issue of whether software is in use when it exists in latent form on a hard drive or is it in use only when present in memory. In a multi-tasking machine, the same software may be loaded into different locations in memory at the same time. An unanswered question of the draft is whether each such copy constitutes a copy for purposes of the software license.

383. U.C.C. § 2-2208(c) (Proposed Draft, Feb. 10, 1995). *See also infra* App. A § 13(c)(ii).

384. *See, e.g.*, U.C.C. § 2-2208(a) (Proposed Draft, Feb. 10, 1995).

385. CLA Survey, *infra* App. B question 2.

386. *See, e.g.*, U.C.C. § 2-2610(c)(2) (Proposed Draft, Feb. 10, 1995).

387. *See, e.g.*, *infra* App. A § 15.

a. Licensor Remedies

In general, licensor remedies will likely turn on whether the nature of the licensee's default is material.³⁸⁸ If a licensee's breach is not material, the licensor may recover damages lost in the ordinary course of business.³⁸⁹ If a licensee's breach is material as to a part of the contract, the licensor may suspend its performance, recover damage to intangibles, recover damages lost for the particular performance, seek specific performance and recover the price.³⁹⁰ If a licensee's breach is material as to the entire contract, the licensor may cancel the contract, terminate rights, repossess and prevent further use, or recover damages as to the entire contract.³⁹¹

b. Licensee Remedies

The licensee's remedies for breach of the license contract by the licensor will also probably turn on whether the breach is material.³⁹² If the licensor's breach is not material, a licensee may not reject the performance as permitted under Article 2's "perfect tender" rule. An aggrieved licensee may, however, seek damages lost in the ordinary course of business, plus consequential damages, obtain recoupment, continue to use the intangibles, or exercise any remedies provided in the contract.³⁹³ If the licensor's default is material as to a part of the contract, the licensee would have the full array of remedies: rejection of the performance; revocation of acceptance; recovery of damages lost in the ordinary course of business; restitution or specific performance; recovery for damage to the value of its intangibles; or suspended performance demanding adequate assurances of performance.³⁹⁴ These same options are available for a licensor's material breach of the entire contract.³⁹⁵

7. MASS-MARKET LICENSES

The enforceability of mass-market licenses is a source of much confusion under current law. The proposed Article 2B will resolve this issue by defining different types of software licenses. Specifically, it will clarify and validate the differences between mass-marketed and

388. See, e.g., U.C.C. § 2-2515 (Proposed Draft, Feb. 10, 1995).

389. See, e.g., U.C.C. § 2-2521 (Proposed Draft, Feb. 10, 1995).

390. See, e.g., U.C.C. § 2-2610(b) (Proposed Draft, Feb. 10, 1995).

391. See, e.g., U.C.C. § 2-2610(a) (Proposed Draft, Feb. 10, 1995).

392. See, e.g., U.C.C. § 2-2603(a) (Proposed Draft, Feb. 10, 1995).

393. See, e.g., U.C.C. § 2-2603 (Proposed Draft, Feb. 10, 1995).

394. See, e.g., U.C.C. § 2-2603(b) (Proposed Draft, Feb. 10, 1995).

395. See, e.g., U.C.C. §§ 2-2603(a), 2-2603(d)(1) (Proposed Draft, Feb. 10, 1995).

customized software. Since various contract rules turn on whether a contract is mass-marketed, this is a critical distinction. The proposed software article will probably define a "mass-market license" as "a standard form license used in a retail or similar transaction in which the licensor does not modify the intangibles specifically for the transaction and the licensee does not sign a written license. The term includes a consumer license."³⁹⁶ This definition comports with the opinions of CLA Survey participants: an overwhelming majority of the respondents identified "mode of distribution" as an important criterion for distinguishing mass-market licenses from other licenses.³⁹⁷ It is also important to distinguish between one-shot transactions and relational contracts.³⁹⁸ Article 2B will recognize this distinction by identifying one-shot transactions as mass-market licenses, distinct from on-going and relational contracts.

The most common mass-market license is the "shrink-wrap"³⁹⁹ agreement. Licensors typically place a printed disclaimer of liability and limitation of remedies underneath the shrink-wrap, assuming that the licensee is bound upon opening the shrink-wrap.⁴⁰⁰ Most

396. U.C.C. § 2-2101 (Proposed Draft, Sept. 10, 1994). A "standard form" license is "a contract prepared by one party in advance for general and repeated use . . . substantially consisting of standard terms and actually used without negotiation of the standard terms with the other party." U.C.C. § 2-102(45) (Proposed Draft, Feb. 10, 1995).

397. Overall, 87% of the CLA Survey respondents agreed that the method of distribution was the best way to separate mass-marketed software from custom software. Sixty-five percent also viewed the form of the license agreement (i.e., shrink-wrap) to be a key criterion for distinguishing mass-marketed from service-oriented software. Additionally, 58% of the survey respondents agreed that the type of end user might also be important in defining mass-marketed software. Only 39% of the computer lawyers believed that mass-marketed software should be defined based upon the number of copies licensed. Only 28% of the respondents viewed price as the key criterion in distinguishing mass-marketed software. CLA Survey, Fall 1994 (see *infra* App. B question 1).

398. Relational contracts involve ongoing relationships where parties have repeat transactions, developing contracting rules through a course of dealing and performance. This ongoing relationship often discourages the parties from becoming involved in litigation. See generally Stewart Macaulay, *An Empirical View of Contract*, 1985 WIS. L. REV. 465 (1985). Stewart Macaulay, *Elegant Models, Empirical Pictures, and the Complexities of Contract*, 11 LAW & SOC'Y REV. 507 (1977). Cf. IAN MCNEIL, *THE NEW SOCIAL CONTRACT* (1980) (describing how parties employ nonlegal mechanisms to enforce relational contracts).

399. Shrink-wrap is the sealed plastic covering of a box containing software.

400. Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2318 n.26 (1994); Mark I. Koffsky, Note, *Patent Preemption of Computer Software Contracts Restricting Reverse Engineering: The Last Stand?* 95 COLUM. L. REV. 1160, 1166 (1995).

mass-marketed software is sold to consumers⁴⁰¹ in retail stores such as Egghead Software, Staples or CompUSA.⁴⁰² Under these conditions, the purchaser must adhere to the terms of the more powerful vendors. These standardized contracts become even more problematic as fewer players dominate the consumer market. Article 2B will account for the commercial reality that mass-marketed software licenses are seldom negotiated. Because requiring a signed and negotiated mass-marketed license agreement would vastly increase transaction costs, the proposed Article 2B will resolve the "unnegotiated" nature of mass-marketed software by validating a standard form license if a licensee—before or within a reasonable time after beginning to use the software—either expressly signs or manifests assent or has the opportunity to review the terms before manifesting assent.⁴⁰³ The emerging software licensing draft will thus conditionally legitimize the "standard form" license.

However, while the proposed Article may resolve the enforceability issue, the standard form license itself remains highly controversial. Merely breaking a shrink-wrap plastic sheet, even if the license terms are visible beforehand, does not connote any real agreement. It is a legal fiction to assume that consumers "agree" to a vendor's limitation of liability. Though there is little empirical research on the effectiveness of shrink-wrap in stemming unauthorized copying of software, it is apparent that shrink-wrap licensing has not solved the problem of unauthorized use.⁴⁰⁴ Moreover, mass-market licenses are presumed to be perpetual,⁴⁰⁵ whereas a non-mass-market license is terminable at will or with reasonable notice.⁴⁰⁶ Nevertheless, some states have enacted statutes providing for the enforcement of shrink-wrap software licenses.⁴⁰⁷ Even a shrink-wrap

401. The proposed Article will likely define both a "consumer" and a "consumer contract." See, e.g., U.C.C. §§ 2-102(11), (12) (Proposed Draft, Feb. 10, 1995) ("A 'consumer contract' means a contract for the sale or license of consumer property between a transferor regularly engaged in the business or selling or licensing and a consumer buyer.").

402. See, e.g., U.C.C. § 2-2101 (Proposed Draft, Feb. 10, 1995).

403. See, e.g., U.C.C. § 2-2203 (Proposed Draft, Feb. 10, 1995).

404. In the mid-1980s, unauthorized copying of software was widespread. One industry estimate was that there were anywhere between 2 and 10 unauthorized copies for every mass marketed software diskette purchased from the publisher. Page M. Kaufman, Note, *The Enforceability of State "Shrink-Wrap" License Statutes in Light of Vault Corp. v. Quaid Software, Ltd.*, 74 CORNELL L. REV. 222, n.2 (1988).

405. See, e.g., U.C.C. § 2-2210(a)(1) (Proposed Draft, Feb. 10, 1995).

406. See, e.g., U.C.C. § 2-2210(b) (Proposed Draft, Feb. 10, 1995).

407. See, e.g., LA. REV. STAT. ANN. § 51:1961-66 (Supp. 1981). During 1985, the state legislatures of California, Georgia and New York introduced but did not pass similar bills.

license which may be enforceable for purposes of contract law may collide with federal intellectual property law.⁴⁰⁸

Although the proposed Article 2B will likely run counter to recent trends against enforceability,⁴⁰⁹ it will only give effect to shrink-wrap agreements if the licensee is given reasonable procedural protection.⁴¹⁰ This strategy corresponds with the opinions voiced by CLA Survey respondents: 65% favored the enforceability of shrink-wrap licenses,⁴¹¹ and most advocated some procedural protection for mass-marketed software.⁴¹² Article 2B's validation of shrink-wrap licenses will clarify the law in favor of the vendor. Consumer advocates and many academics will find this resolution troubling, as it subordinates the interests of consumers to those of large commercial vendors.⁴¹³

408. Mark Lemley presents a compelling case against the enforceability of shrink-wrap licensing in the emergent software licensing law. Professor Lemley writes:

Shrinkwraps are not contracts at all in any meaningful sense of the word. Rather, they are unilateral lists of terms that courts may choose to abide by in some circumstances. Where the court must choose between a shrinkwrap term and creating its own term out of the air, perhaps there is reason to rely on the shrinkwrap But where there is already a federal statute in place that strikes a careful balance in the law, it would be a travesty to disregard that federal law because one party has indicated that it would prefer to have more rights than the law confers.

Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1291-92 (1995); see also Page M. Kaufman, *supra* note 404, at 222-23.

409. See, e.g., *Step-Saver Data System v. Wyse*, 939 F.2d 91, 105 (3rd Cir. 1991) (holding that, because a "box-top"—i.e., shrink-wrap—license agreement substantially altered the distribution of the risk between the buyer and the seller as a matter of law, it did not constitute a final and complete agreement between the parties). See generally Koffsky, *supra* note 400, at 1160.

410. For example, courts will not enforce terms not brought to the licensee's attention or terms that would cause most licensees to refuse the license if the term was brought to their attention. *Id.* However, the proposed law will not require that the licensee actually review the terms of the mass-marketed license. *Id.*

411. The vast majority of attorneys representing both licensors and licensees favor the enforceability of shrink-wrap agreements. Slightly more attorneys representing vendors approved of shrink-wrap agreements. The qualitative portion of the study revealed strong support for procedural protection for mass-marketed shrink-wrap. Many of the respondents questioned the general enforceability of shrink-wrap unless customers were given an opportunity to read and agree to the terms. CLA Survey, Fall 1994 (see *infra* App. B question 5).

412. CLA Survey, Fall 1994 (on file with author).

413. See Lemley, *supra* note 408, at 1252 (discussing cases in which shrink-wrap licenses were found to be "contracts of adhesion" because the consumer lacked a "meaningful choice as to the terms offered").

Article 2B may not dispose of all controversy surrounding the shrink-wrap agreement.⁴¹⁴ However, its balancing of procedural protection with the enforceability of standard form agreements may help to avoid the stalemate between licensors and licensees which has characterized the debate over shrink-wrap licenses.

8. CONCLUSION

In spite of the continuing mass-market license controversy, Article 2B as a whole will make great strides in elucidating the legal landscape of software licensing. For instance, by treating computer software as a license rather than as a good, Article 2B will mold commercial law to fit Internet security software. The proposed Article will also likely clarify the key issues regarding the transfer of security software that are not dealt with in Article 2 and provide much-needed certainty for the developers and constituents of the National Information Infrastructure. Although there is at present only minimal Internet or network case law, it is likely that much future litigation involving Internet security software will revolve around performance standards, warranties and damages. Indeed, the lack of case law is one of the strongest arguments for adopting the proposed Article 2B to provide a uniform starting point to resolve these issues.

B. The Case for Adopting the Proposed Article 2B for Internet Security Software

Lon Fuller wrote that "judges and writers on legal topics frequently make statements they know to be false. These statements are called 'fictions'." ⁴¹⁵ Fuller compared the use of legal "fictions" to a children's game of imagination triggered by "let's play."⁴¹⁶ For the

414. For example, Mark Lemley advocates additional limitations on shrink-wrap licensing. He proposes that the drafters revise Proposed U.C.C. § 2-2203 by augmenting the draft with the following language:

(b) The terms adopted under subsection (a) include all of the terms of the mass-market license without regard to the individual knowledge or understanding of the licensee. However, a term does not become part of the license if the term:

...

(4) creates an obligation or imposes a limitation on the licensee that is inconsistent with federal intellectual property law, or that deprives the licensee of a right or privilege granted the licensee under federal intellectual property law.

Lemley, *supra* note 408, at 1292.

415. LON L. FULLER, *LEGAL FICTIONS* 1 (1967).

416. *Id.*

past decade, courts have pretended that U.C.C. Article 2 applies to the licensing of software. As early as 1988, the court in *Communication Groups, Inc. v. Warner Communications* stated that "it seems clear that computer software, generally, is considered by the courts to be a tangible . . . item."⁴¹⁷ As we have seen, however, software is not tangible. Aside from the physical diskette, software is an intangible collection of magnetically-fixed electronic impulses. Judges are employing a legal fiction when they assume that software is a tangible. Jeremy Bentham would attack this stretching of sales law as a manifestation of the "pestilential breath of Fiction."⁴¹⁸

A "white lie" is also necessary to stretch sales law to the licensing of Internet security products.⁴¹⁹ The vast majority of these products consist entirely or primarily of computer software. They are licensed in a property transfer transaction which is wholly different from sales in both character and result. Von Ihering argued that "[f]ictions are makeshifts, crutches to which science ought not to resort."⁴²⁰

Applying Article 2 to computer software has been a useful fiction. Even Von Ihering acknowledged it is "better that science should go on crutches than to slip without them, or not to venture to move at all."⁴²¹ Nevertheless, the time has come for the courts and Internet security industry to dispense with fictions, white lies and crutches. Article 2B will provide an adequate legal infrastructure for structuring Internet security product transactions. Article 2B will place the law of licensing in accord with commercial and technological realities, clarify ownership dilemmas, approximate more closely international commercial law's tender and performance standards, and accommodate virtually all licensing of intangibles transactions, even continuous-access contracts.

1. CONVERGENCE WITH COMMERCIAL AND TECHNOLOGICAL REALITY

The proposed Article 2B will comport well with commercial practices already existing in the Internet security industry. Licensors

417. *Communication Groups, Inc. v. Warner Communications*, 138 Misc. 2d 80, 83 (N.Y. Civ. Ct. 1988).

418. FULLER, *supra* note 412, at 2 (citing JEREMY BENTHAM, WORKS (1843)).

419. *Id.* at 5 (quoting Von Ihering who called fictions the "white lies" of the law. VON IHERING, GEIST DES ROEMISCHEN RECHTS AUF DEN VERSHIEDENEN STUFEN SEINER ENTWICKLUNG (6th ed. 1924) (The title of this book translates as "The Spirit of Roman Law in the Various Stages of its Development."))

420. *Id.* at 2 (quoting Von Ihering).

421. *Id.*

already negotiate software licensing agreements under the aegis of U.C.C. concepts.⁴²² Contract is the law-in-action being used in marketing Internet security software. For example, licensors grant, limit or disclaim warranties using the prescribed methodology of the U.C.C.⁴²³ Remedies and default terms are negotiated in accordance with U.C.C. principles. A period of acceptance testing is typically built into customized transactions.⁴²⁴ The performance standards of Internet security products are assessed against the benchmark of U.C.C. norms such as good faith, fair dealing and usages of trade. Since mid-century, the U.C.C. has gained hegemony as an influential source of contract law.⁴²⁵ The proposed Article 2B will thus codify commercial practice norms that are already widely accepted.

Article 2B will also adapt U.C.C. standards to the technological realities of Internet security contracting. Given the virtual impossibility of delivering software which contains no errant lines of code, Article 2's perfect tender rule will be replaced by a substantial performance standard. In addition, Article 2's concept of the physical "delivery" of tangibles—which does not fit with the transfer of limited rights in intangible software—will be replaced in the proposed Article 2B with the notion of transfer of rights. The transfer of rights provision will be flexible enough to accommodate transfers of intangibles which occur across electronic media, by remote access or through methods not yet conceived. Moreover, under the proposed Article 2B, the automatic passing of title currently found in Article 2 will be superseded by the provision that the *parties' agreement* will determine the scope of any property rights conveyed in a license transaction. Article 2B will thus eliminate the danger that common law judges could presume that title passes with a license; it will grant licensors default protection not presently assured under common law.⁴²⁶

Furthermore, the proposed Article 2B will address obligations especially applicable to the licensing of Internet security products. These include maintenance and support obligations of the licensor, and

422. See, e.g., *Colonial Life Ins. Co. v. Electronic Data Systems Corp.*, 817 F. Supp. 235, 238-39 (D. N.H. 1993); *Advent Sys. Ltd. v. Unisys Corp.*, 925 F.2d 670, 673-76 (3rd Cir. 1991); *Schroders, Inc. v. Hogan Systems, Inc.*, 137 Misc. 2d 738, 741-42 (N.Y. 1987) (applying warranty law to computer networks). See also *infra* App. A §§ 14-15, 17.

423. See, e.g., *infra* App. A § 14.

424. *Id.*

425. See ALAN SCHWARTZ, *COMMERCIAL TRANSACTIONS: PRINCIPLES AND POLICIES* 2 (1982).

426. Cf. *Sheets v. Yamaha Motors Corp.*, 849 F.2d 179 (5th Cir. 1988) (stating that trade secret protection may be lost by permitting third parties to have access to confidential information).

nondisclosure and confidentiality obligations of both the licensor and licensee. For example, Article 2B will validate a norm of confidentiality for protecting intellectual property commodities.⁴²⁷ Confidentiality is the *sine qua non* of Internet security products.⁴²⁸ The proposed software article would presume that a licensee is not entitled to underlying data or code unless the parties expressly agree to the contrary.⁴²⁹ Furthermore, no assignment may be made that would endanger another party's confidential material.⁴³⁰ A licensee will also not be permitted to resell or transfer materials in its possession after a rightful rejection.⁴³¹ Confidentiality of data and data protection will be so strongly embedded in the new licensing provisions as to survive even dissolution of the contract.⁴³²

Professor Nimmer noted that: "Many intangibles contracts deal with information the value of which is linked to the maintenance of secrecy or confidentiality about the information or technology it describes."⁴³³ Fifty percent of the CLA Survey respondents favored the imposition of a confidentiality obligation on the end-user with respect to non-public information obtained from mass-marketed software.⁴³⁴ The proposed Article 2B will thus recognize and address the well-established concern of confidentiality with respect to the licensing of intangibles such as Internet security products.

2. INTERNATIONALIZATION OF THE INTERNET

Another reason for adoption and use of Article 2B is the growing internationalization of commercial law. The United States is now subject to the United Nations' Convention on Contracts for the International Sale of Goods (CISG).⁴³⁵ If the countries of both parties are signatories to the CISG, then the CISG applies by default and not

427. See, e.g., U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

428. See, e.g., *infra* App. A § 13(c)(ii).

429. See, e.g., U.C.C. § 2-2206 (Proposed Draft, Feb. 10, 1995).

430. See, e.g., U.C.C. § 2-2502 (Proposed Draft, Feb. 10, 1995).

431. See, e.g., U.C.C. § 2-2307 (Proposed Draft, Feb. 10, 1995).

432. See, e.g., U.C.C. § 2-2207 (Proposed Draft, Feb. 10, 1995).

433. U.C.C., Rev. Article 2, Sales, Chapter 3: Licenses, Prefatory Note 10 (Proposed Draft Sept. 10, 1994) (Raymond Nimmer, Reporter).

434. CLA Survey, Fall 1994 (*see infra* App. B question 7).

435. The Convention on Contracts for the International Sale of Goods applies to sales of goods between parties whose places of business are in different states that have signed the Convention. See Convention on Contracts for the International Sale of Goods, 1988, Art. 1 (1), reprinted in COMMERCIAL AND DEBTOR-CREDITOR LAW at 1642 (Douglas G. Baird et al. eds., 1994).

the U.C.C.⁴³⁶ Thus, as more security software is marketed across borders, it is important that American law harmonize with international commercial law. Unfortunately, there are dramatic differences between the U.C.C. and the CISG.⁴³⁷ For example, the CISG does not follow the perfect tender rule of U.C.C. section 2-601. Instead, the CISG has adopted a fundamental breach standard for breach of an obligation, such that a buyer may receive substitute goods only if the delivered goods fundamentally breach the sales contract.⁴³⁸ In contrast, Article 2 permits a buyer to obtain substitute goods if the goods fail "in any respect to conform to the contract."⁴³⁹ These two standards are clearly incompatible.

The proposed Article 2B, on the other hand, is likely to be strikingly similar to the CISG. For example, the proposed Article's concept of substantial performance will likely be functionally equivalent to the CISG's fundamental breach standard. The CISG's definition of "fundamental breach" is: some unexcused failure of performance which "substantially deprives" a party of an entitlement under the contract.⁴⁴⁰ This definition is essentially the "substantial performance" standard of the proposed Article 2B.⁴⁴¹ Therefore, the

436. *Id.* Since the United States is a signatory, CISG applies in any sales transactions with parties of another signatory state. However, Art. 6 of CISG permits the parties to opt out of CISG ("the parties may exclude the application of this Convention"). *Id.* at 1643. The parties may decide to apply the U.C.C. or the proposed Article 2B. In the former case, they may select the law which will govern their rights and duties provided that, in choosing which state's codification applies, they select a jurisdiction which bears a "reasonable relation" to their transaction. U.C.C. § 1-105(1) (1990). In the latter case, the parties will likely be able to select any state's law so long as it does not "contradict fundamental public policy of a more related state." U.C.C. § 2-109(a) (Proposed Draft, Feb. 10, 1995).

437. See generally JOHN HONNOLD, UNIFORM LAW FOR INTERNATIONAL SALES UNDER THE 1980 UNITED NATIONS CONVENTION (2d ed. 1991).

438. Article 25 of the Convention on the International Sale of Goods (CISG) states: A breach of contract committed by one of the parties is fundamental if it results in such detriment to the other party as substantially to deprive him of what he is entitled to expect under the contract, unless the party in breach did not foresee and a reasonable person of the same kind in the same circumstances would not have foreseen such a result.

Convention Relating to a Uniform Law on the International Sale of Goods, July 1, 1964, 834 U.N.T.S. 107, art. 25.

439. See U.C.C. §§ 2-691, 2-711, 2-712 (1990).

440. See generally C.M. BIANCA & M.J. BONELL, COMMENTARY ON THE INTERNATIONAL SALES LAW—THE 1980 VIENNA SALES CONVENTION 205 (1987); JOHN HONNOLD, UNIFORM LAW FOR INTERNATIONAL SALES (1982).

441. See, e.g., U.C.C. § 2-2306 (Proposed Draft, Feb. 10, 1995). Technically, the proposed "hub and spoke" version still allowed jurisdictions to choose either the extant perfect tender rule corresponding to U.C.C. § 2-601 or the substantial performance standard. U.C.C. § 2-2403(b) (Proposed Draft, Feb. 10, 1995). Due to its

juristic truth is that there will be a closer fit between the proposed Article 2B and the norms of the CISG than between Article 2 and CISG. Therefore, adoption of the proposed Article will be one large step closer to harmonization of American and international commercial software law.

The CISG, however, does not explicitly address software licensing. Like Article 2, the CISG is designed for tangible goods and can only apply to the licensing of intangibles by analogy. Further, the CISG does not address problems of contract formation. Essentially, the CISG is a barrier to creating a uniform international body of law for the licensing of intangibles just as Article 2 is a barrier to creating a uniform American software licensing law.

A uniform commercial law of the Internet that applies no matter where the parties reside must be formulated. It should remove barriers to trade and facilitate commercial transactions across the Internet. Although uniform proposals for software protection have been put forth in recent years as part of the General Agreement on Tariffs and Trade (GATT) and in the Council of the European Communities Directive on the Protection of Computer Programs, they are limited in scope.⁴⁴² The ideal solution would be to formulate a new Convention for Software Licensing on the Internet that would provide uniform rules governing transnational Internet contracts, and would be tailored to take into account radically different social, economic and legal systems. The proposed Article 2B might be considered as a possible model since it will provide the vocabulary and the concepts for dealing with intangibles.

3. FLEXIBILITY AND DETERMINACY IN THE LAW

The principal argument for adopting the proposed Article 2B will be its flexibility. Mark Lemley notes that "technological development in the computer industry has outrun the pace of legal

impracticability, however, the perfect tender option is not expected to remain in the final version of Article 2B.

442. See General Agreement on Tariffs and Trade—Multilateral Trade Negotiations (The Uruguay Round): Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Part II, § 1 (Dec. 15, 1993). GATT has limited application because agreements under GATT apply only between governments. *Id.* at Part I. The Council of the European Communities Directive on the Protection of Computer Programs is limited because it applies only to "computer programs" and "preparatory design work" leading to computer programs. *Preamble*, The Council of the European Communities Directive on the Protection of Computer Programs, 1991 O.J. (L 122) 42.

change."⁴⁴³ The proposed Article will offer resolution to this problem. In addition, the accommodation of commercial law to Internet and network security software has the potential of providing comprehensive coverage of licensing to other intangibles and intellectual property as well.

The proposed Article 2B will likely encompass "intangibles contracts and agreements incidental to intangible contracts, including agreements to support, maintain or modify software."⁴⁴⁴ Internet security transactions are often a mixture of sales, licenses and services. These transactions will be treated under the proposed Article, with the exception of the sales aspects of such transactions, which will continue to be treated under Article 2. The scope of the proposed Article, however, will conceivably cover all information licensing contracts.

For example, the proposed software article's reach will likely be broad enough to encompass even continuous access contracts⁴⁴⁵ such as those for the services of CompuServe, Prodigy, America Online, WESTLAW and LEXIS.⁴⁴⁶ Security software will be increasingly marketed to provide privacy and confidentiality when using on-line services. Article 2B will establish specialized default rules tailored for those services, and for other continuous-access contracts.⁴⁴⁷ Most notably, access availability and resolution of disputes with regard to OSPs will be set by usage of trade.⁴⁴⁸ Thus, the proposed software licensing article's recognition of trade usage as a standard is consistent with the U.C.C.'s goal of codifying accepted business practices.⁴⁴⁹

443. Mark A. Lemley, *Convergence in the Law of Software Copyright?*, 10 HIGH TECH. L.J. 1,3 (1995).

444. U.C.C. § 2-2102 (Proposed Draft, Feb. 10, 1995).

445. *See id.*

446. The proposed Article 2B will likely define a "continuous access contract" as a: contract that transfers a right or privilege to have access over a period of time to an intangible, resource, data system, or other facility under the control of the licensor or a third party, and gives the transferee a right of access at a time substantially of its own choosing subject to limitations on the general availability of the intangible, resource, data system or other facility.

U.C.C. § 2-102(13) (Proposed Draft, Feb. 10, 1995).

447. One of the norms will be that access "be available at times and in a manner consistent with . . . express commitments in the contract," or consistent with industry standards. U.C.C. § 2-2314(a) (Proposed Draft, Feb. 10, 1995).

448. For example, neither isolated failures nor scheduled downtime for maintenance will place the OSP licensor in breach. *See, e.g.*, U.C.C. §§ 2-2314 (b), (c) (Proposed Draft, Feb. 10, 1995).

449. One of the key concepts of the U.C.C. is the use of prevailing industry customs to shape contract interpretation and remedies. *See* U.C.C. § 1-205(2) (1994).

There is a widespread feeling in the industry that the law of software contracting is indeterminate. In the CLA Survey, respondents emphasized the need for certainty and clarification of the law of intangibles. Article 2B will address these concerns. The proposed Article's capacity to advance, accommodate and protect changing technologies is precisely why it will be the appropriate template for intangibles. Adoption of the proposed Article for licensing of intangibles will reduce the uncertainty of litigating the potential applicability of an Article 2 provision that is at odds with the more delimited transfer of intellectual property rights. Although not perfect, the proposed Article 2B provides a model of default rules and gap-fillers for parties to either adopt or draft around. It will go a long way toward simplifying, clarifying and modernizing the law governing Internet security products and all licensing of intangibles.

The exact terms of Article 2B are still in flux. The drafters recognize that, in order for software law reform to be effective, they must engineer consensus among diverse stakeholders, such as software industry representatives, U.C.C. stakeholders and consumers. They also must balance the interests of licensors, licensees, consumers, third parties and the public. The drafters are attempting to ensure that these numerous interests and issues will be addressed. For example, care has been taken to establish clear ground rules for a three-party relationship that arises in the intangibles contracting context. The objective is to balance the goals of contract law with the provision of appropriate incentives to minimize the risk of injury.

The proposed Article 2B is an entirely new paradigm that has been specifically drafted for licensing. It substitutes commercial and technological realities for legal fictions. The proposed software licensing article provides a comprehensive, yet flexible, framework upon which all the parties—licensors and licensees, vendors and vendees, merchants, and consumers—may build and structure their Internet security transactions.

V. CONCLUSION

Law does not descend disembodied from the thin, rarefied air of the legal heavens.⁴⁵⁰ The Law of Cyberspace must be forged and molded. It should rely on traditional legal theories only insofar as it produces outcomes which maximize society's benefit in the long run. The legal infrastructure for intangibles must "accommodate itself to

450. Felix S. Cohen, *Transcendental Nonsense and The Functional Approach*, 35 COLUM. L. REV. 809, 809 (1935) (coining the term of the legal heavens "reserved for the theoreticians of the law").

the changing thought and action."⁴⁵¹ During its formative period, especially, the infrastructure must be given some room to develop.⁴⁵²

Like the builders of nineteenth century canals and railroads who benefited from legal doctrines such as the fellow servant rule, contributory negligence and assumption of risk, the builders of the National Information Infrastructure (NII) should be free to contract and allocate liability among themselves and their users. Article 2B affords this freedom of contract to licensors of Internet security products and other intangibles within accepted parameters of good faith and conscionability. The NII is just beginning to emerge. If the NII is saddled with too much tort or statutory liability, its development may be endangered.

Experience rather than logic must guide commercial law.⁴⁵³ The Uniform Commercial Code has been the most successful codification experience in American history. Modernizing the U.C.C. to accommodate Internet security products and intangibles will best facilitate the development of the NII. The proposed Article 2B will accomplish this goal.

451. FOWLER V. HARPER & FLEMING JAMES, JR., *THE LAW OF TORTS* xxvii (1956) (arguing that the law of torts has historically proven to be very adaptable).

452. LAWRENCE M. FRIEDMAN, *A HISTORY OF AMERICAN LAW* 409-27 (1973).

453. Justice Oliver Wendell Holmes' famous aphorism was that the life of the law is experience not logic: "The law embodies the story of a nation's development through many centuries In order to know what it is, we must know what it has been, and what it tends to become." OLIVER W. HOLMES, *THE COMMON LAW* 1 (1881).

APPENDIX A

EXAMPLE OF SALES AND LICENSE AGREEMENT OF A
NETWORK SECURITY PRODUCT

Appendix A provides an example of sales and license agreement for a information security product. This agreement also employs many U.C.C. concepts and methods. For example, there are provisions for warranties, disclaimers, limitations, modification and "sole and exclusive" remedies.

Agreement No.:

COMPANY X
AGREEMENT FOR PURCHASE OF EQUIPMENT
AND LICENSE OF SOFTWARE

This Agreement is made this _____ day of _____, 19____ by and between COMPANY X, a Delaware corporation with its principal place of business at _____ ("XXX"), and the Customer, its affiliates and subsidiaries whose name and address are set forth below (the "Customer").

Name of Customer:

Bill To:

Ship To (if different):

Street

Street

City

City

State Zip Code

State Zip Code

Telephone Number: ()

Telephone Number: ()

Point of Contact:

Point of Contact:

The Customer agrees to purchase and XXX, by its acceptance and execution of this Agreement, agrees to sell and/or license, on the terms and conditions set forth in the Terms and Conditions of Sale and Software License Agreement attached hereto, the equipment, software, firmware and features listed below (the "Products").

Customer:

Company X:

Name

Name

Signed

Signed

Title

Title

TERMS AND CONDITIONS
OF SALE AND
SOFTWARE LICENSE AGREEMENT

The Products sold and/or licensed under this Agreement consist of hardware, software and firmware. Unless otherwise expressly provided in this Agreement, all sales or licenses of Products by XXX are made in accordance with and subject to the following terms and conditions, except that to the extent that the Products constitute software and/or firmware, they are not sold to the Customer but are licensed to the Customer under Section 13 of this Agreement.

1. **Prices.** The Customer may rely only on prices published by XXX or quoted in writing from an authorized XXX representative, which prices may be changed at any time without notice. Written quotations expire automatically thirty (30) calendar days from the date issued and are subject to change or termination by notice during that period. All prices are subject to adjustment on account of specifications, quantities, shipment arrangements or other terms and conditions which are not part of the original price quotation. The purchase prices, license fees and other charges for the Products shall be as set forth in this Agreement or, if no prices have been specified, shall be XXX's established prices in effect at the time of shipment. Unless otherwise expressly stated in writing, all prices are F.O.B. XXX's facility in Cambridge, Massachusetts.

2. **Taxes.** Prices are exclusive of all federal, state, municipal or other excise, sales, use, occupational or similar taxes now in force or enacted in the future, all of which shall be paid by the Customer, except for such taxes as are imposed on XXX's income. XXX may invoice the Customer for any such taxes and remit any payments made on any such invoice directly to the appropriate taxing authorities. The Customer is responsible for obtaining and providing to XXX any certificate of exemption or similar document required to exempt any sale or license from sales, use or similar tax liability.

3. **Terms of Payment.** Unless otherwise expressly stated in writing, payment terms for the Products (together with any invoiced charges for shipping, insurance and applicable taxes) are net thirty (30) days from date of invoice. XXX reserves the right at any time to require full or partial payment in advance, or to revoke any credit previously extended, if, in XXX's judgment, the Customer's financial condition does not warrant proceeding on the terms specified. Overdue payments shall be subject to finance charges computed at a periodic rate (to the extent permitted by law) of 1 1/2% per month (18% per year), plus all costs and expenses, including reasonable attorney's fees, incurred by XXX in collecting such overdue amounts.

4. **Delivery.** The requested delivery date for each of the Products is stated on the second page of this Agreement. XXX will use reasonable efforts to meet requested delivery dates, but does not represent or warrant that it will, in fact, meet such dates, all shipments being subject to XXX's availability schedule. Shipping dates are also based upon prompt receipt of all necessary information from the Customer. XXX shall not be liable for any delay in delivery, or failure to deliver, due to causes beyond its control, including, without limitation, acts of nature, acts or omissions of the Customer, acts of civil or military authority, fires, lockouts, strikes and slowdowns, floods, epidemics, quarantine restrictions, wars, riots, delays in transportation, unavailability of supplies or sources of energy, or delays in delivery by XXX's suppliers. In the event of delay due to any such cause, the time for delivery shall be extended for a period equal to the duration of the delay, and the Customer shall not be entitled to refuse delivery or otherwise be relieved of any obligation as a result of the delay.

5. **Shipment.** Unless specific instructions to the contrary are set forth in this Agreement, XXX will select methods and routes of shipment. XXX will not assume any liability in connection with shipment or constitute any carrier as its agent. All shipments will be insured at the Customer's expense and made at the Customer's risk, and the Customer shall be responsible for making claims with carriers, insurers, warehousemen and others for misdelivery, non-delivery, loss, damage or delay. All transportation, rigging, draying and handling charges, and all insurance costs, shall be paid by the Customer. XXX may, at its option, invoice the Customer for any such charges and remit any payments directly to the shipper and/or insurer.

6. **Title and Risk of Loss.** Subject to the terms set forth in Section 7 below and to XXX's right to stop delivery of Products in transit, title to and risk of loss for Products shall pass to the Customer upon the earlier of delivery (a) to the Customer or (b) to a carrier for shipment to the Customer; provided, however, that title to the Software and User Documentation (as such terms are defined in Section 13 of this Agreement) shall at all times remain with XXX.

7. **Security Interest.** As security for the payment and performance by the Customer of all of its liabilities and obligations under this Agreement, the Customer hereby grants to XXX a security interest in the Products (together with their products and proceeds, including all credit, fire or other insurance proceeds). The Customer acknowledges that a copy of this Agreement may be filed with the appropriate authorities as a financing statement in order to evidence the security interest granted to XXX. In addition, the Customer agrees to execute and deliver such financing statements and other documents as XXX requests to perfect the security interest granted hereby.

8. Cancellations.

(a) Cancellation of Standard Orders. Except as set forth in paragraph (b) below, the Customer may cancel any order for Products under this Agreement at any time before shipment without the payment of any cancellation charge. If any order is canceled by the Customer after shipment of the Products, then (i) the Customer shall pay the cost of shipment to the Customer's site and the cost of returning any such Products to XXX, (ii) risk of loss shall remain with the Customer until such Products have been returned to XXX, and (iii) the Customer shall pay an administrative fee of \$150 to XXX for each such canceled order.

(b) Cancellation of Non-Standard Orders. In the event that the Customer cancels a non-standard order at any time prior to shipment, then the Customer agrees to pay the full price of any (i) custom applications, as described on the second page of this Agreement, and (ii) completed components, sub-assemblies and/or finished assemblies (which may include full production runs) of non-standard Products (i.e., Products fabricated to meet the Customer's requirements, drawings, specifications or other designs). No cancellations shall be permitted after non-standard Products have been shipped.

9. Installation. Unless otherwise specified in this Agreement, the Customer assumes sole responsibility for the installation of Products at the Customer's premises.

10. Specifications. All products are subject to XXX's standard tolerances for specifications. XXX reserves the right to make substitutions and modifications in the specifications of any Products; provided, that such substitutions or modifications do not materially adversely affect the performance of the Products or the purposes for which they can be used.

11. Use of Data. Any specifications, drawings, technical information or other data furnished by XXX to the Customer shall remain the property of XXX, shall be kept confidential by the Customer, and shall be returned to XXX promptly upon XXX's request.

12. Claims for Non-Conforming Shipments. All claims for non-conforming shipments must be made in writing to XXX within ten (10) days of delivery of goods to the Customer. Any claims not made within that period shall be deemed waived and released.

13. Software License.

(a) Definitions. For purposes of this Agreement:

(i) "Host System" shall mean the hardware and other computer equipment in connection with which the Products are utilized, as set forth on the second page of this Agreement.

(ii) "User Documentation" shall mean the manuals, handbooks and other written materials relating to the Software and the Products provided by XXX to the Customer.

(iii) "Software" shall mean all software and firmware, including all computer programs, whether in the form of tape, disk, ROM or other memory storage, incorporated in or used in connection with the Products and provided by XXX to the Customer, consisting of a series of instructions or statements in machine-readable, object code form only, and all modifications, refinements and improvements thereto made by XXX which XXX provides to the Customer.

(b) Grants of License. XXX hereby grants, and the Customer hereby accepts, a royalty-free, non-exclusive, nontransferable license, without the right to sublicense, subject to the terms and conditions of this Agreement, to use the Software on and in connection with the Host System and to utilize the User Documentation, for the Customer's internal purposes only. No right or license is granted under this Agreement for the use or other utilization of the Software, directly or indirectly, for the benefit of any other person or entity or in conjunction with any equipment other than the Host System.

(c) Ownership, Intellectual Property Rights and Non-Disclosure.

(i) Title to and ownership of the Software, including patents, copyrights and property rights applicable thereto, shall at all times remain solely and exclusively with XXX, and the Customer shall not take any action inconsistent with such title and ownership.

(ii) The Customer shall not cause or permit disclosure, copying, display, loan, publication, transfer of possession (whether by sale, exchange, gift, operation of law, or otherwise) or other dissemination of the Software or User Documentation, in whole or in part, to any third party without the prior written consent of XXX. The Customer shall take all reasonable steps to safeguard the Software and User Documentation and to ensure that no unauthorized persons have access to the Software and User Documentation, and that no persons authorized to have such access shall take any action which would be prohibited by this Agreement if taken by the Customer. The Customer shall promptly report to XXX any actual or suspected violation of this clause (ii) and shall take such further steps as may reasonably be requested by XXX to prevent or remedy any such violation.

(iii) The Customer shall include and shall not alter or remove any copyright, trade secret, proprietary and/or other legal notices contained on or in the Products, Software and User Documentation. The existence of any such copyright notice on the Products, Software or User Documentation shall not be construed as an admission, or deemed to create a presumption, that publication of such material has occurred.

(iv) The Customer shall promptly respond to all reasonable inquiries by XXX concerning the Customer's compliance with the provisions of this paragraph (c) of this Section 13.

(d) Acknowledgment of No Program Rights. The Customer acknowledges that XXX is the owner of the Software and the User Documentation for purposes of Section 117 of the Copyright Act of 1976, as amended, and for all other purposes, and that XXX intends that the Customer will use the Software and the User Documentation only in accordance with the terms and conditions of this Agreement. Physical copies of the Software and the User Documentation shall be deemed to be on loan to the Customer during the term of the license granted hereunder.

(e) Modification of Software. The Customer shall not modify, enhance or otherwise change or supplement the Software without the prior written consent of XXX.

(f) Term of License. XXX may terminate the license of the Software granted hereunder, by written notice to the Customer, if the Customer fails to comply with any of the terms or conditions of this Agreement. Within ten (10) days after any termination of this license hereunder, the Customer shall destroy or return to XXX the original and all copies (including partial copies) of the Software and the User Documentation and shall certify in writing to XXX that it has done so. The Customer shall pay any shipping and handling charges necessary to return the Software and the User Documentation to XXX. Any further obligations of the parties shall cease upon termination of this Agreement; provided, that the terms and conditions of Sections 11, 15, 16 and 18 and paragraph (c) of this Section 13 shall continue in full force and effect for a period of five (5) years following the termination of this Agreement.

14. Warranty.

(a) Equipment.

(i) XXX warrants that the Products (to the extent not constituting Software) shall in all material respects be free from defects in material and workmanship for a period of ninety (90) days from the date of shipment. Any claims of defects not made within such 90-day period shall be deemed waived and released.

XXX's sole obligation with respect to claims of defects made within the warranty period described above shall be, at its option, to repair or replace any item which it determines to be defective, either at XXX's facility or the Customer's facility, at the discretion of XXX. All transportation charges to such facility will be prepaid by the Customer, and XXX will pay all return transportation charges. XXX may employ used parts to make repairs or replacements, so long as the used parts are not defective in any respect and are of a quality equivalent to new parts. All replaced parts will become the property of XXX on an exchange basis.

(ii) All Card Modules are guaranteed, unless subjected to unreasonable use or physical abuse, for the purchased life set forth on the second page of this Agreement, to functionally perform in conformity with XXX product literature in all material respects, including physical integrity, battery life, functional integrity, and synchronization with the Products so long as XXX implementation requirements are maintained for use on the Host System.

(b) Software. During the first ninety (90) days following shipment of the Software, XXX will, upon receipt of a problem report from the Customer, correct all documented code errors determined by XXX to be such and caused by a defect in an unaltered version of the Software delivered to the Customer. Any claims of nonconformance which are not made within such 90-day period shall be deemed waived and released. XXX's sole obligation with respect to claims of nonconformance shall be to remedy the nonconformance (either by repair or replacement, at XXX's option) when reported to it by the Customer. This warranty shall not apply (i) if the Software has been modified or altered by the Customer and (ii) in the event that repair or replacement cannot be made or is ineffective due to the operational characteristics of any Host System.

(c) Limitations of Warranty. The foregoing warranty shall not apply if (i) repair or replacement is required as a result of causes other than normal use, including, without limitation, repair, maintenance, alteration or modification of the Products by persons other than XXX or other XXX-authorized personnel, accident, fault or negligence of the Customer, operator error or improper use or misuse of the Products, or causes external to the Products such as, but not limited to, failure of electrical power or fire or water damage; or (ii) the Products are modified by the Customer or used with software or equipment other than the Host System. The Customer acknowledges and accepts responsibility for his or its selection of the Products to achieve the Customer's intended results, for his or its use of the Products and for the results obtained thereby. The Customer also accepts responsibility for the selection and use of, and the results obtained from, any other equipment, software or services used in conjunction with the Products. XXX's liability for damages to the Customer for any cause, regardless of the form of action, shall not exceed the aggregate price paid for the Products under this Agreement.

(d) No action, whether in contract or tort, including negligence, arising out of or in connection with this Agreement, may be brought by either party more than two years after the cause of action has accrued. This paragraph (d) shall not apply to actions for any breach of the provisions of Section 17 or actions by XXX for violations or infringements of XXX's rights relating to the Software licensed hereunder.

OTHER THAN AS SET FORTH IN THIS SECTION 14, XXX DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE PRODUCTS (INCLUDING, WITHOUT LIMITATION, WARRANTIES AS TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE), EITHER EXPRESS OR IMPLIED, AND THE FOREGOING EXPRESS WARRANTIES ARE IN LIEU OF ALL LIABILITIES OR OBLIGATIONS ON THE PART OF XXX. IN NO EVENT WILL XXX BE LIABLE FOR LOSS OF USE, DATA OR PROFITS, OR OTHER SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF ANY PRODUCTS, EVEN IF XXX HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

15. **Limitation of Liability.** The express obligations contained in this Agreement are in lieu of all liabilities or obligations of XXX for damages, including, but not limited to, general, special or consequential damages arising out of or in connection with the delivery, use or performance of the Products, Software and/or User Documentation, or arising from the negligence of XXX, its employees, officers, directors, or consultants. In addition, the Customer further agrees that:

(a) In no event will XXX be liable to the Customer for lost profits or similar damages or for any claims against the Customer by any other party; and

(b) XXX's liability to the Customer for damages resulting from any cause whatsoever shall be limited to the charges paid by the Customer for use of the Products, Software and/or User Documentation, as the case may be, relating to the cause of such damages.

16. **Documentation.** All documentation with respect to the Products, including, without limitation, training documentation, software documentation and maintenance manuals and drawings, is furnished solely for the Customer's internal use. The Customer may make copies of such documentation to satisfy its internal requirements, provided that all such copies include copyright and proprietary information notices. No other copies or use of such documentation, or any portion thereof, shall be made without the prior written approval of XXX.

17. **Patent and Copyright Indemnity.** If notified promptly in writing of any action (and provided that XXX has been promptly notified of all prior claims relating to such action) brought against the Customer based on a claim that the

current, unaltered release of the Products, Software or User Documentation supplied to the Customer infringes a United States patent or copyright, XXX shall defend such action at its expense and pay any costs or damages finally awarded in such action which are attributable to such claim, provided that XXX shall have sole control of the defense of any such action and all negotiations for its settlement or compromise. If a final injunction is obtained against the Customer's use of any of the Products, Software or User Documentation by reason of infringement of a United States patent or copyright, or if in XXX's opinion any of the Products, Software or User Documentation supplied to the Customer hereunder is likely to become the subject of a successful claim of infringement of a United States patent or copyright, XXX shall, at its option and expense, either procure for the Customer the right to continue using such Products, Software or User Documentation, as the case may be, or replace or modify the same so that it becomes non-infringing, or grant the Customer a credit for such Products, Software or User Documentation, as the case may be, and accept its return. Notwithstanding the foregoing, XXX shall not have any liability to the Customer under this Section 17 if the infringement or claim is based upon (i) the use of any of the Products, Software or User Documentation in combination with other equipment or software which is not furnished by XXX, (ii) Products, Software or Product Documentation which have been modified or altered by the Customer, or (iii) the furnishing to the Customer of any information, service or application assistance. The Customer shall indemnify and hold XXX harmless against any expense, judgment or loss for infringement of any patents, copyrights or trademarks as a result of XXX's compliance with the Customer's designs, specifications or instructions. No cost or expenses shall be incurred for the account of XXX without the prior written consent of XXX. IN NO EVENT SHALL XXX'S TOTAL LIABILITY TO THE CUSTOMER UNDER THIS SECTION 17 EXCEED THE AGGREGATE SUM PAID TO XXX BY THE CUSTOMER FOR THE ALLEGEDLY INFRINGING EQUIPMENT OR PROGRAM. THE FOREGOING STATES THE ENTIRE LIABILITY OF XXX WITH RESPECT TO INFRINGEMENT OF PATENTS OR COPYRIGHTS BY ANY OF THE PRODUCTS, SOFTWARE OR USER DOCUMENTATION OR ANY PART THEREOF OR THEIR OPERATION.

18. Injunctive Relief. Because unauthorized use or transfer of the Software or User Documentation, or any information contained therein, may diminish substantially the value of such materials and may irrevocably harm XXX, if the Customer breaches the provisions of Sections 11 or 16 or paragraph (c) of Section 13 of this Agreement, XXX shall (without limiting its other rights or remedies) be entitled to equitable relief (including but not limited to injunctive relief) to protect its interests and, if the Customer has not returned the Software and the User Documentation to XXX, or certified to XXX's satisfaction that the Software and the User Documentation have been destroyed, XXX shall have the right to enter and take possession of the Software and the User Documentation wherever located without liability for damage, so long as XXX shall have acted reasonably and in good faith.

19. Notices. All notices given by either party to the other party under this Agreement shall be in writing and personally delivered or sent by registered or certified mail, return receipt requested, to the other party at its address set forth above. The date of personal delivery or the date of mailing, as the case may be, shall be deemed to be the date on which such notice is given.

20. General.

(a) The obligations of XXX under this Agreement shall be subject to the procurement by, and at the expense of, the Customer of any import or export licenses, documents, permits or clearances required with respect to this Agreement and are subject to the condition precedent that all necessary approvals from governmental authorities have been obtained. The Customer agrees at all times to comply with all laws of the United States of America and its 50 states applicable to the Customer and shall not take, or refrain from taking, any action which would result in the violation of such laws by XXX. Nothing contained in this Agreement shall be construed as creating a joint venture, partnership or employment relationship between the parties.

(b) The validity, construction and interpretation of this Agreement and the rights and duties of the parties hereto shall be governed by and construed in accordance with the laws of The Commonwealth of Massachusetts.

(c) This Agreement constitutes the entire understanding between the Customer and XXX with respect to the subject matter hereof, and XXX makes no representations to the Customer except as expressly set forth herein.

(d) Terms and conditions set forth in any purchase order or other document provided by the Customer to XXX which differ from, conflict with or are not included in this Agreement shall not be part of any agreement between XXX and the Customer unless specifically accepted by XXX in writing. To the extent that this document may constitute an acceptance, such acceptance is expressly conditioned on the Customer's assent to any additional or inconsistent terms and conditions set forth in this document.

(e) This Agreement shall not be deemed or construed to be modified, amended or waived, in whole or in part, except by written agreement of the parties hereto.

(f) The Customer may not assign this Agreement, or any of its rights or obligations hereunder, without the prior written consent of XXX.

(g) Section headings are for descriptive purposes only and shall not control or alter the meaning of this Agreement.

(h) All rights and remedies of either party shall be cumulative and may be exercised singularly or concurrently. The failure of either party, in any one or more instances, to enforce any of the terms of this Agreement shall not be construed as a waiver of future enforcement of that or any other term.

(i) If any provision of this Agreement shall for any reason be held illegal or unenforceable, such provision shall be deemed separable from the remaining provisions of this Agreement and shall in no way affect or impair the validity or enforceability of the remaining provisions of this Agreement.

(j) XXX shall not be liable for failure to fulfill any of its obligations under this Agreement due to causes beyond its control.

SCHEDULE OF PRODUCTS

1. Description of Products

Qty	Model	Description	Price
-----	-------	-------------	-------

3. Total Purchase

Price:	\$
--------	----

Taxes:	\$
--------	----

Shipping:	\$
-----------	----

TOTAL:	\$
--------	----

(due net thirty days from date of invoice)

4. Requested Delivery Date:

5. Host System:

Manufacturer

Model

Serial No.

Operating System

Location

APPENDIX B

COMPUTER LAW ASSOCIATION SURVEY AND RESULTS

This survey was mailed to all 950 members of The Computer Law Association in August of 1995. The membership consists of intellectual property attorneys who develop, distribute and use computer technology. We received 147 responses to the survey which represented a 15% response rate. For more information regarding the survey and respondents, see note 305.

Reproduced below is the text of the survey questions and the answers from which the respondents could choose. The bracketed numbers represent the total number of respondents (not the percentage) who selected that particular answer. Neither the space provided for commentary nor the actual comments are reproduced here. All comments made by respondents are on file with co-author Michael Rustad.

Survey results were compiled by Elaine Martel.

I. GENERAL INFORMATION ABOUT RESPONDENT

A. Which category best describes your background?

(Check the single, most appropriate, box)

Consumer, not a business	[0]
Software	[44]
High tech electronics (hardware)	[16]
Chemicals	[1]
Legal services	[69]
Financial services	[1]
Consumer products	[1]
Government/public	[2]
Academic	[2]
Medical distributor	[1]
Utility	[0]
Service industry	[8]
Other (please identify)	[0]

B. The size of your 1992 sales were approximately:

\$1 million to under \$10 million	[21]
\$10 million to under \$100 million	[25]
\$100 million to under \$1 billion	[17]
Over \$1 billion	[17]

C. Your business involvement with software is primarily as a:

(Check All Boxes Appropriate)

Purchaser/licensee of software	[70]
Seller/licensor of software owned by your company	[55]
Reseller of software	[18]
Consultant	[84]
Software developer	[38]
Service bureau	[8]

D. You work primarily with:

(Check All Boxes Appropriate)

Custom developed or customized software	[109]
Industry specific software	[104]
Mass marketed software	[87]
Horizontal system software	[7]
Other (please identify)	[0]

E. Your function primarily is:

(Check All Boxes Appropriate)

Sales	[0]
Purchasing	[0]
Information systems	[0]
Software developer	[0]
Consumer	[0]
Legal	[all]
Other (please identify)	[0]

F. Personal info:

(Check All Boxes Appropriate)

Male	[127]
Female	[20]
Attorney	[all]
Sales	[0]
Other	[0]
Under 5 years involvement with software	[70]
5—15 years involvement with software	[95]
Over 15 years involvement with software	[45]

G. In your software transactions, what type of agreements do you often use?

(Check All Boxes Appropriate)

Signed license agreement or development agreement	[132]
Unsigned "shrink wrap" license	[91]
Purchase order	[58]
Electronic license (without written agreement)	[24]
No formal agreement	[17]
Detailed contracts supplementing license terms	[97]
Other (please identify)	[0]

H. For which types of agreements do you frequently obtain legal review of software agreements before signing?

(Check All Boxes Appropriate)

Signed license agreement or development agreement	[103]
Unsigned "shrink wrap" license	[31]
Purchase order	[23]
Electronic license (without written agreement)	[14]
No formal agreement	[7]
Detailed contracts supplementing license terms	[76]
Other (please identify)	[0]

II. SUBSTANTIVE QUESTIONS

1. DEFINITION

Mass marketed software should be defined:

	Agree	No Opinion	Disagree
Based on number of copies licensed to date	[42]	[20]	[66]
Based on method of distribution	[104]	[11]	[16]
Based on the type of end user	[57]	[24]	[42]
Based on form of license agreement (e.g., license agreements that did not provide for signatures by the parties would automatically qualify)	[72]	[17]	[39]
Based on price	[28]	[25]	[72]

2. ASSIGNABILITY

Regardless of any shrink wrap license restrictions, the law should allow the end user to:

	Agree	No Opinion	Disagree
Assign or resell software	[83]	[11]	[49]
Move the physical location of software	[122]	[2]	[19]
Use software forever	[73]	[16]	[52]
Resell rightfully rejected software to recover costs	[45]	[23]	[70]
Assign software to an outsourcing vendor (a company hired to manage data processing activities; software may need to be moved, run at a different location, etc.)	[79]	[15]	[46]

3. WARRANTY

The following warranties should be included with all shrink wrap software and MAY NOT BE DISCLAIMED:

	Agree	No Opinion	Disagree
The software vendor has the right to license the software product	[127]	[5]	[13]
The software vendor has no knowledge of infringement of any third party rights	[105]	[13]	[27]
The software product does not infringe any third party proprietary rights	[69]	[22]	[53]
The software product will operate substantially in accordance with its accompanying user documentation	[110]	[10]	[24]
The software product contains no expiration dates or disabling routines	[58]	[27]	[58]
The software product contains no viruses, worms [or] other malicious routines	[74]	[34]	[43]
The software product contains no routines to prevent unauthorized use	[22]	[35]	[85]

4. WARRANTY

The following warranties should be included with all shrink wrap software UNLESS CONSPICUOUSLY DISCLAIMED by the seller:

	Agree	No Opinion	Disagree
The software vendor has the right to license the software product	[63]	[11]	[55]
The software vendor has no knowledge of infringement of any third party rights	[56]	[18]	[54]
The software product does not infringe any third party proprietary rights	[46]	[20]	[64]
The software product will operate substantially in accordance with its accompanying user documentation	[75]	[8]	[46]
The software product contains no expiration dates or disabling routines	[64]	[17]	[54]
The software product contains no viruses, worms [or] other malicious routines	[50]	[19]	[64]
The software product contains no routines to prevent unauthorized use	[54]	[20]	[61]

5. SCOPE OF RIGHTS GRANTED*The law should provide that:*

	Agree	No Opinion	Disagree
Shrink wrap licenses are enforceable contracts	[85]	[14]	[45]

6. SCOPE OF RIGHTS GRANTED*Regardless of any shrink wrap license provisions, the end user should have the right to:*

	Agree	No Opinion	Disagree
Load and execute the software on a single computer	[141]	[0]	[5]
Make back-up copies	[138]	[2]	[5]
Reverse engineer the software to determine & exploit underlying non-copyrightable ideas	[52]	[18]	[76]
Load software on a network file server and make it available to a single user at a time	[91]	[15]	[38]
Load software on a network file server and make available to an unlimited number of users	[5]	[19]	[120]
Load software on a network and make available to users for a usage fee	[33]	[21]	[90]

7. SCOPE OF RIGHTS GRANTED*Regardless of any shrink wrap provisions, shrink wrap software should:*

	Agree	No Opinion	Disagree
Impose an obligation of confidentiality on the end user with respect to non-public information obtained from the software	[61]	[22]	[60]

In the following hypothetical situations please respond based on your view of what the applicable law should be.

8. HYPOTHETICAL

A consumer purchases shrink-wrap software, uses the software for one year, then sells the software and documentation. The consumer does not maintain a copy of the software after it is sold.

Statement—Regardless of any shrink-wrap license restrictions against the “rental, resale, or transfer,” a buyer should have the right to resell the shrink-wrap software.

For	Against	No Opinion
[97]	[43]	[6]

9. HYPOTHETICAL

Detailed shrink wrap license conditions state that the software may not be “rented, sold or transferred”.

Statement—The purchaser should be able to install this software on a computer, even if this computer is rented to patrons for \$10.00 per hour.

For	Against	No Opinion
[47]	[82]	[16]

10. HYPOTHETICAL

A consumer purchases entertainment software. The software is shrink wrap software and contains a variety of disabling routines designed to permit use of the software only until Dec. 31, 1994. The company also sells a perpetual license of the same product at a higher cost.

Statement—If the software is conspicuously labeled, the seller should be able to include disabling routines and enforce shrink wrap license restrictions designed to grant non-perpetual software license.

For	Against	No Opinion
[120]	[18]	[7]

11. HYPOTHETICAL

A consumer buys a new furnace which contains software designed to control furnace performance. The software contains disabling routines which render the furnace inoperable unless the consumer pays an annual maintenance fee for service and updates to the software. This restriction is clearly labeled on the furnace and spelled out in shrink-wrap license restrictions.

Statement—By conspicuous labeling, a seller should be able to include disabling routines and enforce non-perpetual license restrictions for software embedded in, or designed to work with, other products.

For	Against	No Opinion
[61]	[75]	[9]

12. HYPOTHETICAL

A business purchases this furnace in order to develop alternate software by reverse engineering the furnace and the software. New software is developed which does not violate any patents or copyrights.

Statement—Regardless of any shrink-wrap license restrictions included with the furnace prohibiting “reverse engineering, decompiling, or disassembly of the software”, the business should be able to license use of this newly developed software.

For	Against	No Opinion
[80]	[49]	[16]

13. SOFTWARE “SPOKE” OF THE PROPOSED UCC

Have you heard about the newly proposed software “spoke” for Article Two of the UCC?

Yes	No
[58]	[86]

ARTICLE

LENDING THE FEDERAL CIRCUIT A HAND: AN ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS

TIMOTHY J. DOUROS †

TABLE OF CONTENTS

I.	INTRODUCTION	322
II.	PROVISIONS AND PURPOSES OF THE PATENT ACT.....	324
	A. Constitutional and Statutory Basis.....	324
	B. Goals of the American Patent System.....	325
III.	INFRINGEMENT AND THE DOCTRINE OF EQUIVALENTS	326
	A. Infringement Generally.....	326
	B. Infringement Under the Doctrine of Equivalents	327
IV.	ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS	330
	A. The Hand Formula	331
	B. Transformation of the Hand Formula: The Economic Doctrine of Equivalents	332
	C. Criticisms and Strengths of the Economic Doctrine of Equivalents.....	345
V.	APPLICATION OF THE ECONOMIC DOCTRINE OF EQUIVALENTS	348
	A. Application Generally	348
	B. Application to <i>Graver Tank</i>	350
VI.	CONCLUSION	352

© 1995 Timothy J. Douros.

† Associate, Morgan & Finnegan, L.L.P., New York; J.D., 1995, Boston College; A.B., 1990, Dartmouth College.

I. INTRODUCTION

The Court of Appeals for the Federal Circuit was created,¹ in part, to bring uniformity to judicial rulings in the area of patent law.² Nowhere in the patent law is such uniformity more needed than in application of the doctrine of equivalents.³ Since the Supreme Court gave the doctrine modern acceptance in *Graver Tank & Manufacturing Co. v. Linde Air Products Co.*,⁴ application of the doctrine has been a source of controversy for courts,⁵ scholars,⁶ and practitioners.⁷

In *Graver Tank*, the Supreme Court held that where an accused device does not literally infringe the claims of the patentee's device, infringement may be found under the doctrine of equivalents, if the accused device performs *substantially* (1) the same function (2) in the

1. The U.S. Constitution, Article III, § 1, provides for the creation of "such inferior Courts as the Congress may from time to time ordain and establish."

2. Federal Courts Improvement Act of 1982, Pub. L. No. 97-164, 96 Stat. 25; see also S. REP. NO. 275, 97th Cong., 2d Sess. 11 (1982), reprinted in 1982 U.S.C.C.A.N. 11, 11 (stating that the statute is "part of a comprehensive program designed to improve the quality of our Federal court system.") The Act withdrew the jurisdiction of the twelve regional Courts of Appeals.

3. The veracity of this statement is partially due to the Federal Circuit's efficacy in clarifying other areas of the patent law. See generally Rochelle Cooper Dreyfuss, *The Federal Circuit: A Case Study in Specialized Courts*, 64 N.Y.U. L. REV. 1 (1989); Douglas A. Strawbridge et al., *Patent Law Developments in the United States Court of Appeals for the Federal Circuit During 1986*, 36 AM. U. L. REV. 861 (1987).

4. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605 (1950).

5. See, e.g., *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1545 (Fed. Cir. 1995) (en banc) (Plager, J., dissenting) (stating that the majority failed "to bring a consistent and rationalized practice to the doctrine of equivalents"); *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 939 (Fed. Cir. 1987) (en banc) (Bennett, J., dissenting) (accusing the majority of "contraven[ing] Supreme Court precedents . . . [and] rewrit[ing] the doctrine of equivalents without regard for stare decisis principles"); *Graver Tank*, 339 U.S. at 613 (Black, J., dissenting) (stating that the majority opinion "steriliz[es] . . . Acts of Congress and prior decisions").

6. See, e.g., Martin J. Adelman & Gary L. Francione, *The Doctrine of Equivalents in Patent Law: Questions that Pennwalt Did Not Answer*, 137 U. PA. L. REV. 673, 728-29 (1989) (arguing that justice would best be served if the doctrine of equivalents were abandoned); Timothy L. Tilton, *The Doctrine of Equivalents in Patent Cases*, 32 J. PAT. OFF. SOC'Y 861 (1950) (predicting that the Supreme Court would use *Graver Tank* to abolish the doctrine of equivalents).

7. See, e.g., Rudolph P. Hofmann, Jr., *The Doctrine of Equivalents: Twelve Years of Federal Circuit Precedent Still Leaves Practitioners Wondering*, 20 WM. MITCHELL L. REV. 1033, 1060 (1994) ("uncertainty remains in every issue of the doctrine of equivalents as currently applied"). Tom Arnold, of Arnold, White & Durkee, observed that different panels of the Federal Circuit "have gone off on frolics of their own in an effort to render the doctrine narrower and more specific. And they have generated one hell of a turmoil, with opinions that don't reconcile with each other." Victoria Slind-Flor, *Rethinking Protection: Software Patents, Copyright Issues Shaped the IP Landscape in '93*, NAT'L L.J., Jan. 24, 1994, at S27.

same way (3) to achieve the same result.⁸ Judge Plager described judicial frustration with the doctrine of equivalents thusly:

[One] problem with the doctrine is that appellate review of many of these doctrine of equivalents cases is largely pro forma. Federal district judges, perhaps understandably, by and large make little pretense of liking these patent infringement cases, and are quite content to give them, and all the issues in them, to juries to decide. The cases typically come to us on appeal with nothing more than a general verdict finding infringement. There is no explanation by the jury of the rationale behind their verdict, if any exists.⁹

Recently, the Federal Circuit restated the test for infringement under the doctrine of equivalents.¹⁰ In *Hilton Davis*, the court sought to enunciate a formulation of the doctrine of equivalents that is both consistent with the tripartite test described in *Graver Tank* and amenable to proper application by trial courts. Specifically, the Federal Circuit held that "application of the doctrine of equivalents rests on the substantiality of the differences between the claimed and accused products or processes, assessed according to an objective standard."¹¹ Thus, the standard for equivalency is insubstantial difference between the accused device and the patent claim.¹² Further, the court held that the function/way/result test of *Graver Tank* is but one method of demonstrating insubstantial difference.¹³ In addition, the majority resisted the temptation to delimit application of the doctrine of equivalents by, for example, rendering it an equitable remedy¹⁴ or requiring an element of intent.¹⁵ Finally, the *Hilton Davis* court, by stating that "the doctrine of equivalents provides the same protection to the substance of the claim scope provided by the doctrine of literal infringement,"¹⁶ has reaffirmed the proposition that "[a]pplication of the doctrine of equivalents is the exception, . . . not the rule, for if the public comes to believe (or fear) that the language of patent claims can never be relied on, . . . then claims will cease to serve their intended purpose."¹⁷

8. 339 U.S. at 608-09.

9. *Hilton Davis*, 62 F.3d at 1538 (Plager, J., dissenting).

10. *Id.* at 1516.

11. *Id.* at 1518.

12. *Id.*

13. *Id.*

14. *Id.* at 1521.

15. *Id.* at 1519.

16. *Id.* at 1528.

17. *London v. Carson Pirie Scott & Co.*, 946 F.2d 1534, 1538 (Fed. Cir. 1991).

This article describes an economic equation, modeled after the Hand Formula,¹⁸ that addresses both the goals of the Patent Act and the purpose of the doctrine of equivalents. In addition to addressing these concerns, the equation, which is referred to in this article as the Economic Doctrine of Equivalents, removes some of the subjectivity of the traditional doctrine of equivalents and provides for greater ease of judicial application. The equation may be used for two different, but related, purposes. First, it may be used to analyze and explain judicial interpretation of the doctrine of equivalents from an economic perspective. Second, the equation serves as a guide to future judicial application of the doctrine of equivalents by providing judges with a framework for evaluating the most important considerations of the doctrine of equivalents and a method for applying those considerations to a particular case.

Part II of this paper examines the Patent Act and its purposes, in order to elucidate the underlying policies and concerns of patent protection. Part III examines infringement in general, and the doctrine of equivalents in particular, in light of the policy goals of the Patent Act. Part IV describes the elements of the Economic Doctrine of Equivalents. Part V discusses the application of the Economic Doctrine of Equivalents and applies it to the facts of *Graver Tank* to demonstrate the consistency of the economic formulation with the aims of the traditional analysis under the doctrine of equivalents. Part VI is the conclusion.

II. PROVISIONS AND PURPOSES OF THE PATENT ACT

Any consideration of the doctrine of equivalents must begin with an examination of the patent system generally. Moreover, proper application of any interpretation of the doctrine of equivalents requires an understanding of the purposes of the Patent Act.¹⁹ In this way, courts, attorneys and scholars may avoid a construction of the doctrine of equivalents that is inconsistent with the Patent Act.

A. Constitutional and Statutory Basis

The Constitution of the United States grants Congress the power "[t]o promote the . . . useful Arts, by securing for limited Times to . . . Inventors the exclusive Right to their . . . Discoveries."²⁰ This

18. *United States v. Carroll Towing*, 159 F.2d 169 (2d Cir. 1947).

19. The current patent statute is 35 U.S.C. §§ 1-376 (1988).

20. U.S. CONST. art. I, § 8, cl. 8.

constitutional provision gave rise to the first Patent Act in 1790.²¹ While the Patent Act has been revised numerous times since the first act, the patent system has remained substantially the same since 1836.

B. Goals of the American Patent System

In the broadest sense, the American patent system is designed to provide an economic incentive for technological advancement and investment in scientific research.²² Furthermore, by requiring full disclosure of the subject matter to be patented, the system provides for dissemination of information that is critical to further technological advances. The patent system encourages both invention and investment, and presumes that consequential benefits, in the form of wealth and information, will accrue to society.²³ The patent is an economic reward which allows the inventor to exclude others from manufacturing, using, or selling the invention for a limited period of time. Given the widespread antipathy toward monopolies²⁴ that existed at the time the Constitution was drafted, the Founding Fathers must have had a strong belief that the patent system, though potentially harmful, would result in an overall benefit to society.²⁵

21. An Act to promote the progress of useful Arts, ch. 7, 1 Stat. 109 (1790) (repealed 1793).

22. See, e.g., Robert P. Merges & Richard R. Nelson, *On the Complex Economics of Patent Scope*, 90 COLUM. L. REV. 839 (1990) (detailing the economic benefits that result from the patent system).

23. But see FRIEDRICH A. VON HAYEK, *THE FATAL CONCEIT: THE ERRORS OF SOCIALISM* (1989); Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity*, 61 AM. ECON. REV. 561 (1971).

24. A patent, of course, is not a monopoly. As then-Chief Judge Markey observed, "[i]t is but an obfuscation to refer to a patent as 'the patent monopoly' or to describe a patent as an exception to the general rule against monopolies." *Schenck, A.G. v. Norton Corp.*, 713 F.2d 782, 786 n.3 (Fed. Cir. 1983). However, given the development of the patent law from the English law of monopolies, the tradition of mischaracterizing a patent as a monopoly is understandable. The Case of Monopolies, *Darcy v. Allin*, 77 Eng. Rep. 1260 (K.B. 1602), was the first English case to declare a royal patent grant void as contrary to the common law and in violation of many acts of Parliament. Later, in *The Clothworkers of Ipswich*, *Godbolt*, 252, 78 Eng. Rep. 147 (K.B. 1615), the court recognized that while the Crown did not have power to grant a monopoly in a specific trade, it could grant an exclusive right for a limited time to an inventor who introduced a new discovery. Later, in 1623, Parliament enacted the Statute of Monopolies, 21 Jam. ch. 3, which served both to codify the common law and provide a statutory basis for the British patent law. See generally Edward C. Walterscheid, *The Early Evolution of the United States Patent Law: Antecedents* (pts. 1 & 2), 76 J. PAT. & TRADEMARK OFF. SOC'Y 697, 849 (1994).

25. Thomas Jefferson, an inventor and member of the commission created by the 1790 Patent Act to oversee the patent system, observed that only those "things which are worth to the public the embarrassment of an exclusive patent" deserve patent

The modern view of the patent system, backed by substantial economic analysis,²⁶ is not qualitatively different from the views held by the drafters of the Constitution. The basic notion that the patent system provides an incentive to invent and invest, outweighing the dangers of monopoly, is still the prevailing view.²⁷ Much recent criticism of the patent system focuses on the inefficient allocation of resources to "block" alternative patentable methods in order to preserve the value of one's patent.²⁸ Because these efforts contribute nothing substantial to society's technological understanding or aggregate wealth, patent protection is unwarranted. Therefore, the patent system ideal is to provide incentives for invention and investment in areas that will be useful to society, while minimizing the effects of inefficient allocation of resources that result from duplicative, insubstantial research.

III. INFRINGEMENT AND THE DOCTRINE OF EQUIVALENTS

A. Infringement Generally

The Patent Act provides that "whoever without authority makes, uses or sells any patented invention, within the United States during the term of the patent therefor, infringes the patent."²⁹ In determining whether an accused device³⁰ infringes a patent, either

protection. *Graham v. John Deere Co.*, 383 U.S. 1, 10-11 (1966). James Madison concluded that the public good resulting from a patent grant coincided with the inventor's right to the invention and that the individual states could not effectively regulate the matter. THE FEDERALIST NO. 43, at 288 (James Madison) (Jacob E. Cooke ed., 1961).

26. See, e.g., Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977); WILLIAM D. NORDHAUS, INVENTION, GROWTH, AND WELFARE: A THEORETICAL TREATMENT OF TECHNOLOGICAL CHANGE (1969); Yoram Barzel, *Optimal Timing of Innovations*, 50 REV. ECON. & STAT. 348 (1968); John S. McGee, *Patent Exploitation: Some Economic and Legal Problems*, 9 J.L. & ECON. 135 (1966); F.M. SCHERER ET AL., PATENTS AND THE CORPORATION (2d ed. 1959); Arnold Plant, *The Economic Theory Concerning Patents for Inventions*, 1 ECONOMICA 30 (1934).

27. For an excellent discussion of intellectual property generally and government incentives to technological progress, see Edmund W. Kitch, *Property Rights in Inventions, Writings and Marks*, 13 HARV. J.L. & PUB. POL'Y 119 (1990).

28. See, e.g., SUBCOMMITTEE ON PATENTS, TRADEMARKS AND COPYRIGHTS, SENATE COMM. ON THE JUDICIARY, 85TH CONG., 2D SESS., AN ECONOMIC REVIEW OF THE PATENT SYSTEM 15 (Comm. Print 1958) (Fritz Machlup).

29. 35 U.S.C. § 271(a) (1988).

30. As used in this article, the word "device" means any patentable subject matter under 35 U.S.C. § 101 (1988).

literally or under the doctrine of equivalents, a court must ascertain the meaning and limits of the patentee's claims and then apply those claims to the accused device.³¹ This determination is made for both literal infringement and infringement under the doctrine of equivalents.³² Literal infringement occurs when an accused device incorporates all of the claims of the patented device.³³

B. Infringement Under the Doctrine of Equivalents

1. THEORETICAL BASIS OF THE DOCTRINE OF EQUIVALENTS

The doctrine of equivalents is a judicial construction which recognizes the frailties of the written word.³⁴ Because, as one scholar has noted, "[a]n infringer appropriates an invention, not words,"³⁵ infringement may occur even though the accused device does not directly infringe upon the literal words of the patentee's claims. To deny recovery for infringement by a device that does not literally infringe upon the claims of a patent, but which nonetheless imitates the patented device, "would be to convert the protection of the patent grant into a hollow and useless thing."³⁶ A court may consider infringement under the doctrine of equivalents only after it has determined that there is no literal infringement.³⁷

31. *Key Mfg. Group, Inc. v. Microdot, Inc.*, 925 F.2d 1444, 1448 (Fed. Cir. 1991); *Palumbo v. Don-Joy*, 762 F.2d 969, 974 (Fed. Cir. 1985); *Texas Instruments, Inc. v. United States Int'l Trade Comm'n*, 805 F.2d 1558, 1568-70 (Fed. Cir. 1986) [hereinafter *Texas Instruments I*].

32. *Texas Instruments I*, 805 F.2d at 1568-70; *SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985); *Martin v. Barber*, 755 F.2d 1564, 1567 (Fed. Cir. 1985).

33. *Laitram Corp. v. Rexnord, Inc.*, 939 F.2d 1533, 1535 (Fed. Cir. 1991); *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1580 (Fed. Cir. 1989); *Julien v. Zeringue*, 864 F.2d 1569, 1571 (Fed. Cir. 1989).

34. *See Winans v. Denmead*, 56 U.S. (15 How.) 330, 343 (1853) (observing that "where the whole substance of the invention may be copied in a different form, it is the duty of courts and juries to look through the form for the substance of the invention"); *Zeigler v. Philips Petroleum Co.*, 483 F.2d 858 (5th Cir.), *cert. denied*, 414 U.S. 1079 (1973) (recognizing the doctrine of equivalents as a safeguard against the elevation of form over substance); *cf. Cabell v. Markham*, 148 F.2d 737, 739 (2d Cir. 1945) (Judge Hand noting that "it is one of the surest indexes of a mature and developed jurisprudence not to make a fortress out of the dictionary"). *But cf. White v. Dunbar*, 119 U.S. 47, 51 (1886) (warning that a patent claim is not "like a nose of wax which may be turned and twisted in any direction").

35. 1A LESTER HORWITZ, *PATENT OFFICE RULES AND PRACTICE* § 111.6 (1992).

36. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 607 (1950).

37. *Id.* at 607-08. However, there is no equitable threshold for application of the doctrine of equivalents. "The doctrine of equivalents has no equitable or subjective

2. APPLICATION OF THE DOCTRINE OF EQUIVALENTS

In *Graver Tank*, the Supreme Court established a tripartite test for infringement under the doctrine of equivalents by stating that the doctrine is predicated on the theory that "if two devices do the same work in substantially the same way, and accomplish substantially the same result, they are the same, even though they differ in name, form, or shape."³⁸ The *Graver Tank* Court considered two electric welding compositions.³⁹ The patented composition was a combination of alkaline earth metal silicate and calcium fluoride.⁴⁰ The accused composition used silicates that were not of an alkaline earth metal.⁴¹ In all other respects, the compositions were identical.⁴² The Court relied on the prior art to establish that persons skilled in the art would have understood that the accused composition could be substituted for (i.e., was equivalent to) the claimed composition.⁴³ Therefore, the doctrine of equivalents was applied to prevent the accused device from fraudulently circumventing the patent.⁴⁴ The rationale behind the doctrine, the Court said, is that "one may not practice a fraud on a patent."⁴⁵ Simply put, the doctrine prevents a person from circumventing a patent by use of an equivalent means, if that means would have been obvious to one skilled in the art of the patent.

The method for determining equivalency to a claim or limitation of the patented device varies depending on the facts of a specific case.⁴⁶ Some cases hold that the focus must be on the combination as a whole,⁴⁷ while others indicate that an equivalent of every claim limitation must be found in the accused device.⁴⁸ In either case, the

component." *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1523 (Fed. Cir. 1995) (en banc).

38. *Graver Tank*, 339 U.S. at 608 (quoting *Machine Co. v. Murphy*, 97 U.S. 120, 125 (1877)).

39. *Graver Tank*, 339 U.S. at 610.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.* at 611-12.

44. *Id.* at 612.

45. *Id.* at 608.

46. *Malta v. Schulmerich Carillons, Inc.*, 952 F.2d 1320, 1326 (Fed. Cir. 1991) ("How equivalency . . . is met necessarily varies from case to case due to many variables such as the form of the claim, the nature of the invention defined by it, the kind of limitation that is not literally met, etc.").

47. *Texas Instruments I*, 805 F.2d 1558, 1568-70 (Fed. Cir. 1986).

48. *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 934-36 (Fed. Cir. 1987) (en banc).

appropriate comparison is between the accused device and the patent claim, not simply a comparison of the two devices.⁴⁹

3. PIONEER INVENTIONS

In the case of a pioneer invention,⁵⁰ the patented device is entitled to broad protection under the doctrine of equivalents.⁵¹ This broad protection arises from the dearth of relevant prior art, rather than an expansive interpretation of the patent claims.⁵² Conversely, a patented device that constitutes only a slight improvement in an area of substantial prior art will receive limited protection against infringement under the doctrine.⁵³

4. RESTRICTIONS ON THE DOCTRINE OF EQUIVALENTS

The two major restrictions on the doctrine of equivalents are "prosecution history estoppel"⁵⁴ and limits imposed by the prior art.⁵⁵ Under prosecution history estoppel, a patentee is estopped from asserting infringement of claims which are embodied in the accused device but were rejected during prosecution of the patentee's patent.⁵⁶ The purpose of this doctrine is to prevent the patentee from benefiting from claims that were clearly rejected by the Patent Office and are not within the scope of the patent.⁵⁷ The range of equivalents to

49. *Read Corp. v. Portec, Inc.*, 970 F.2d 816, 822 n.2 (Fed. Cir. 1992). The court provided the example of the comparison between a pencil and a pen: while the two "may for many purposes or uses be generally equivalent, . . . claim limitations drawn to a pen would not under the doctrine of equivalents cover a pencil and vice versa." *Id.*

50. The Supreme Court defined a pioneer invention as "a wholly novel device, or one of such novelty and importance as to mark a distinct step in the progress of the art, as distinguished from a mere improvement or perfection of what had gone before." *Westinghouse v. Boyden Power Brake Co.*, 170 U.S. 537, 562 (1898). More simply, a pioneer invention is an invention without significant prior art. *Texas Instruments I*, 805 F.2d at 1572.

51. *Morley Sewing-Mach. Co. v. Lancaster*, 129 U.S. 263, 272-84 (1889); *Perkin-Elmer Corp. v. Westinghouse Elec. Corp.*, 822 F.2d 1528, 1532 (Fed. Cir. 1987) (citing *Sealed Air Corp. v. United States Int'l Trade Comm'n*, 645 F.2d 976, 984 (C.C.P.A. 1981)).

52. *Texas Instruments v. United States Int'l Trade Comm'n*, 846 F.2d 1369, 1370 (Fed. Cir. 1988).

53. *Hughes Aircraft Co. v. United States*, 717 F.2d 1351, 1362 (Fed. Cir. 1983).

54. This is alternatively known as file wrapper estoppel. *Amstar Corp. v. Envirotech Corp.*, 730 F.2d 1476, 1485 (Fed. Cir. 1984).

55. *Stewart-Warner Corp. v. City of Pontiac, Mich.*, 767 F.2d 1563, 1572 (Fed. Cir. 1985).

56. *Schriber-Schroth Co. v. Cleveland Trust Co.*, 311 U.S. 211, 220-21 (1940); *Black & Decker, Inc. v. Hoover Serv. Ctr.*, 866 F.2d 1285, 1295 (Fed. Cir. 1989).

57. *Mannesmann Demag Corp. v. Engineered Metal Prods. Co.*, 793 F.2d 1279, 1284 (Fed. Cir. 1986).

which a claimed invention is entitled is also limited in that it may not include what was prior art when the patent was prosecuted.⁵⁸

A further restriction on the doctrine of equivalents is the "reverse doctrine of equivalents." As the *Graver Tank* Court noted, if "a device is so far changed in principle from a patented article that it performs the same or similar function in a substantially different way, but nevertheless falls within the literal words of the claim, the doctrine of equivalents may be used to restrict the claim and defeat the patentee's action for infringement."⁵⁹ Thus, where an invention relies on the fundamental concept embodied in a patent but is more sophisticated than the patented device due to "a significant advance," the accused device does not infringe by virtue of the reverse doctrine of equivalents.⁶⁰ Once a patentee establishes literal infringement, the burden is on the alleged infringer to establish noninfringement under the reverse doctrine of equivalents.⁶¹

The symmetry of the doctrine of equivalents and the reverse doctrine of equivalents extends to their faults as well. That is, if it is difficult to determine whether a device is not substantially different from a patented device such that there is infringement, it will not be much easier to determine whether a device that falls within the literal words of the claim is so substantially different that infringement does not occur.

IV. ECONOMIC INTERPRETATION OF THE DOCTRINE OF EQUIVALENTS

Patent infringement may be thought of as a federal law tort.⁶² Although this analogy is inapposite in some circumstances,⁶³ similarities between patent infringement and tort law render the

58. *Stewart-Warner*, 767 F.2d at 1572.

59. *Graver Tank*, 339 U.S. at 608-09.

60. *Mead Digital Sys., Inc. v. A.B. Dick Co.*, 723 F.2d 455, 464 (6th Cir. 1983).

61. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1123-24 (Fed. Cir. 1985).

62. *See, e.g., Beverly Hills Fan Co. v. Royal Sovereign Corp.*, 21 F.3d 1558, 1570-71 (Fed. Cir. 1994) (for purposes of a state's long-arm statute, the situs of the tort of patent infringement is not the domicile of the patentee but the place where the allegedly infringing activity takes place); *A.C. Aukerman Co. v. R.L. Chaides Constr. Co.*, 960 F.2d 1020, 1031 (Fed. Cir. 1992) (laches is an appropriate defense to continuing torts, such as patent infringement); *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1579 (Fed. Cir. 1986) (infringement is a tort for purposes of corporate liability); *Carbice Corp. v. Am. Patents Dev. Corp.*, 283 U.S. 27, 33 (1931) ("[i]nfringement, whether direct or contributory, is essentially a tort").

63. *See, e.g., North Am. Philips Corp. v. Am. Vending Sales, Inc.*, 35 F.3d 1576, 1579 (Fed. Cir. 1994) ("[W]hile it may be appropriate to speak loosely of patent infringement as a tort, more accurately the cause of action for patent infringement is created and defined by statute.").

former amenable to analysis incorporated in the latter. The level of *mens rea* required, the remedies available and the general economic impact all facilitate infringement analysis by traditional tort law methods.⁶⁴ Therefore, the following analysis and transformation of tort law principles, guided by patent law purposes, is a logical extension of economic analysis into the realm of the patent law.

A. The Hand Formula

In 1947, Judge Learned Hand first posited a framework for an economic interpretation of negligence. In *United States v. Carroll Towing*,⁶⁵ Judge Hand recognized the economic considerations involved in determining whether a party has acted reasonably.⁶⁶ A person's duty to protect against injuries resulting from his behavior is determined by relating: (1) the probability that the injury will occur; (2) the magnitude of the resulting injury; and (3) the burden of taking precautions to prevent the injury from occurring.⁶⁷ Judge Hand asserted that liability for injury resulting from certain action attaches when the burden (B) is less than the product of the probability (P) and the magnitude of the injury (L).⁶⁸ This relationship is summarized in a simple algebraic formula as $B < P \cdot L$.⁶⁹ When the burden of preventing the accident is greater than the product of the probability and magnitude of the injury ($B > P \cdot L$), the actor has not acted negligently and arguably should not be liable for any injury resulting from his actions.

The rationale for this approach is that tort law should encourage economically desirable behavior.⁷⁰ As Judge Posner observed:

When the cost of accidents is less than the cost of prevention, a rational profit-maximizing enterprise will pay tort judgments to the accident victims rather than incur the larger cost of avoiding liability. Furthermore, overall economic value or welfare would

64. See generally RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* (4th ed. 1992); WERNER Z. HIRSCH, *LAW AND ECONOMICS* (2d ed. 1988).

65. 159 F.2d 169 (2d Cir. 1947).

66. See generally Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 32 (1972).

67. *Carroll Towing*, 159 F.2d at 173.

68. *Id.*

69. While the formula may be simple, the conceptual and practical application may not be. Judge Hand himself recognized the problems that may arise in applying the test: "The difficulties are in applying the rule, . . . they arise from the necessity of applying a quantitative test to an incommensurable subject matter; and the same difficulties inhere in the concept of 'ordinary' negligence." *Moisan v. Loftus*, 178 F.2d 148, 149 (2d Cir. 1949).

70. Posner, *supra* note 66, at 32-33.

be diminished rather than increased by incurring a higher accident-prevention cost in order to avoid a lower accident cost. If, on the other hand, the benefits in accident avoidance exceed the costs of prevention, society is better off if those costs are incurred and the accident is averted, and so in this case the enterprise is made liable, in the expectation that self-interest will lead it to adopt the precautions in order to avoid a greater cost in tort judgments.⁷¹

Thus, by this view, tort law should not deter activity by attaching liability where the cost of preventing any resulting injury exceeds the cost of the injury itself. In this way, the law promotes economic efficiency.

B. Transformation of the Hand Formula: The Economic Doctrine of Equivalents

By considering the purposes of the patent law in general, and of the doctrine of equivalents in particular, it is possible to design an equation similar in nature to the Hand Formula that may be used to determine infringement under the doctrine of equivalents. Commercial viability, in conjunction with investment and obviousness considerations, may be used directly in considering infringement under the doctrine of equivalents.⁷² These concepts may be related in an equation to facilitate application of the doctrine of equivalents. According to the formulation, an accused device does not infringe under the doctrine of equivalents when its obviousness (O), as measured by investment (reflected in the prior art) in the problem addressed by the accused device,⁷³ is less than the product of direct investment (I) in the accused device⁷⁴ and the commercial viability (C_v) of the accused device, defined as the increased efficiency, measured in dollars, created by the accused device.⁷⁵ Thus, where $O < C_v \cdot I$, there is no infringement under the doctrine of equivalents. Conversely,

71. *Id.* at 33.

72. One author has suggested that commercial viability could distinguish a recombinant protein from the naturally occurring isolate by creating a legal fiction whereby a recombinant protein would be "coupled" to its method of production. Michael S. Greenfield, *Recombinant DNA Technology: A Science Struggling with the Patent Law*, 44 STAN. L. REV. 1051, 1082 (1992). The Economic Doctrine of Equivalents gives greater meaning to the concept of commercial viability so that it may be applied in all cases where the issue of infringement under the doctrine of equivalents is raised.

73. The definition of the term "obviousness," as used in this article, is discussed in greater detail *infra* text accompanying notes 81-123.

74. The definition of the term "investment," as used in this article, is discussed in greater detail *infra* text accompanying notes 124-130.

75. The definition of the term commercial viability, as used in this article, is discussed in greater detail *infra* text accompanying notes 131-139.

where the obviousness of the accused device is greater than the product of investment and commercial viability ($O > C_V \cdot I$), the device infringes under the doctrine of equivalents.

In *Hilton Davis*, the Federal Circuit emphasized the importance of the substantiality of differences between the accused device and the patent claims.⁷⁶ In determining the substantiality of the differences, the factfinder must consider "objective evidence rather than unexplained subjective conclusions."⁷⁷ Objective evidence of equivalency is not limited to the function/way/result test of *Graver Tank*, but includes any evidence relevant to the substantiality of the differences between the accused device and the patent claim.⁷⁸ In fact, the Federal Circuit stated that "neither the Supreme Court nor this court limits the types of evidence that either party may proffer in support of a factor it considers probative of infringement under the doctrine."⁷⁹ The court recognized that "the presence of such factors will depend on the way parties frame their arguments."⁸⁰ By incorporating the objective evidence of obviousness, investment in the accused device and commercial viability, the Economic Doctrine of Equivalents examines evidence that is probative of infringement under the doctrine of equivalents. Thus, the Economic Doctrine of Equivalents is a suitable means for determining equivalency under the doctrine of equivalents.

Obviousness, investment and commercial viability, as used in the Economic Doctrine of Equivalents, will next be discussed in some detail. Although the following analysis describes use of the factors in a quantitative sense, the analysis may be conducted qualitatively as well. Like the Hand Formula, the Economic Doctrine of Equivalents may be used as a construct to clarify the criteria that a court will consider in determining infringement under the doctrine of equivalents.

1. OBVIOUSNESS

Obviousness is an underlying concern of the doctrine of equivalents. Indeed, obviousness is a synonym for the "insubstantial differences" standard enunciated by the Federal Circuit in *Hilton*

76. *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1518 (Fed. Cir. 1995) (en banc).

77. *Id.* at 1519.

78. *Id.* at 1518.

79. *Id.* at 1522.

80. *Id.*

Davis.⁸¹ The Federal Circuit has described obviousness under 35 U.S.C. § 103 as analogous to infringement under the doctrine of equivalents.⁸² The *Graver Tank* Court stated that, when determining equivalence, "[a]n important factor is whether persons reasonably skilled in the art would have known of the interchangeability of an ingredient not contained in the patent with one that was."⁸³

The obviousness factor (O) ensures that only significant improvements to a patented device will be found not to infringe under the Economic Doctrine of Equivalents. The concept of obviousness used in the Economic Doctrine of Equivalents might be described as an economic test of obviousness, and differs from the obviousness concept used in determining patentability. It should be clear that I do not advocate the use of the economic test of obviousness as a standard for patent validity. Obviousness with respect to patent validity addresses whether or not patent protection is initially appropriate; the Economic Doctrine of Equivalents, in contrast, is concerned with economic investment and with the economic impact of patents and accused devices. In the following two parts, nonobviousness in the context of patentability and in the Economic Doctrine of Equivalents are each considered.

a. Nonobviousness as a requirement for patentability

The traditional test of nonobviousness is required by section 103 of the Patent Act. Section 103 provides:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.⁸⁴

This language was explicated by the Court in *Graham*,⁸⁵ which stated:

81. *Id.* at 1520. The court further explained that "those who make only insubstantial changes to a patented product or process are liable for infringement, regardless of their awareness of the patent and its disclosure." *Id.*

82. In explaining the difference between the definition of "anticipation" before and after the 1952 amendment of the Patent Act, Judge Nies observed that "[a]ll infringements of a device do not 'anticipate' [the device] . . . Some may be infringements under the doctrine of equivalents which, if one wished to draw a parallel, is somewhat akin to obviousness." *Lewar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 748 (Fed. Cir. 1987).

83. *Graver Tank*, 339 U.S. at 609.

84. 35 U.S.C. § 103 (1988).

85. *Graham v. John Deere Co.*, 383 U.S. 1 (1966).

the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.⁸⁶

According to this test, "[o]bviousness is a legal conclusion based on factual determinations and not a factual determination itself."⁸⁷ The necessary factual determinations are: (1) the scope and content of the prior art; (2) the differences between the prior art and the invention; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness.⁸⁸ For each of these factual determinations, the inquiry must focus, as the statute requires, on "the time the invention was made."⁸⁹ That is, a court must conclude whether the claimed invention *would have been* obvious to a person of ordinary skill at the time the invention was made, not at the time of trial.⁹⁰

Under section 103, determination of obviousness requires an examination of the "art to which [the] subject matter pertains."⁹¹ The pertinent art is determined by examining the nature of the problem confronting the inventor,⁹² as well as by considering the type of skill required to understand the patent in question, and the type of art applied to the claims by the Patent Office.⁹³ Before determining the scope and content of the pertinent prior art, a court must determine whether a reference is prior art.⁹⁴ Once this legal requirement is met,

86. *Id.* at 17-18.

87. *Aktiebolaget Karlstads Mekaniska Werkstad v. United States Int'l Trade Comm'n*, 705 F.2d 1565, 1575 (Fed. Cir. 1983) (citing *General Motors Corp. v. United States Int'l Trade Comm'n*, 687 F.2d 476, 480 (Fed. Cir. 1982), *cert. denied*, 459 U.S. 1105 (1983)).

88. *See Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1535-40 (Fed. Cir. 1983).

89. 35 U.S.C. § 103 (1988).

90. *See Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1570-71 (Fed. Cir.), *cert. denied*, 481 U.S. 1052 (1987).

91. 35 U.S.C. § 103 (1988).

92. *See Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 620 (Fed. Cir.), *cert. dismissed*, 474 U.S. 976 (1985).

93. *See Orthopedic Equip. Co., Inc. v. United States*, 702 F.2d 1005, 1008 (Fed. Cir. 1983).

94. *See Panduit*, 810 F.2d at 1568. What the prior art comprises, as contrasted with what it teaches, is a question of law. *General Motors Corp. v. United States Int'l Trade Comm'n*, 687 F.2d 476, 482 n.10 (C.C.P.A. 1982), *cert. denied*, 459 U.S. 1105 (1983). Sources of prior art are mentioned in 35 U.S.C. § 102 and include prior

the court must follow certain legal standards to determine the scope and content of the prior art.⁹⁵

The factfinder must determine whether "the reference is within the field of the inventor's endeavor."⁹⁶ If so, the reference is within the scope of the prior art.⁹⁷ If not, the factfinder must then determine "whether the reference is reasonably pertinent to the particular problem with which the inventor was involved."⁹⁸ According to the Federal Circuit, a "reference is reasonably pertinent if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering [the] problem."⁹⁹ This consideration requires the factfinder to determine whether a person having ordinary skill in the art¹⁰⁰ would reasonably have expected to solve the problem facing the inventor by considering the reference in question.¹⁰¹

Before determining the differences between the prior art and the invention, the court must interpret the meaning and scope of the

knowledge or use, prior patents, prior publications, description in a prior copending patent application that ripens into a patent, prior invention, and derivation from another. 2 CHISUM, PATENTS § 5.03[3] (1994). However, "section 102 is not the *only* source of section 103 prior art." *In re Fout*, 675 F.2d 297, 300 (C.C.P.A. 1982).

95. See *Panduit*, 810 F.2d at 1568. For example, when the prior art reference is a patent, the "patent must be considered in its entirety, i.e., as a *whole*, including portions that would lead away from the invention in suit . . . ; elements of separate prior patents cannot be combined when there is no suggestion of such combination anywhere in those patents . . . and a court should avoid hindsight" *Id.* (citations omitted).

96. *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 449 (Fed. Cir. 1986).

97. See, e.g., *In re Deminski*, 796 F.2d 436, 442 (Fed. Cir. 1986).

98. *Bausch & Lomb*, 796 F.2d at 449.

99. *In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992). The court further observed:

Thus, the purposes of both the invention and the prior art are important in determining whether the reference is reasonably pertinent to the problem the invention attempts to solve. If a reference disclosure has the same purpose as the claimed invention, the reference relates to the same problem, and that fact supports use of that reference in an obviousness rejection. An inventor may well have been motivated to consider the reference when making his invention. If it is directed to a different purpose, the inventor would accordingly have had less motivation or occasion to consider it.

Id.

100. The concept of a "person with ordinary skill in the art" is discussed in greater detail *infra*, text accompanying notes 106-110.

101. *Clay*, 966 F.2d at 660.

patent claims at issue.¹⁰² This interpretation is a question of law, incorporating "the objective test of what one of ordinary skill in the art at the time of the invention would have understood the term to mean."¹⁰³ The court must consider the claimed "subject matter as a whole," rather than merely compare the claimed subject matter with the prior art.¹⁰⁴ The differences must be evaluated in terms of the whole invention, including whether or not the prior art contains "some teaching, suggestion, or incentive" to make the changes that produce the claimed invention.¹⁰⁵

In determining obviousness, section 103 requires reference to a hypothetical person of ordinary skill in the art.¹⁰⁶ This person is "presumed to be one who thinks along the line of conventional wisdom in the art and is not one who undertakes to innovate, whether by patient, and often expensive, systematic research or by extraordinary insights."¹⁰⁷ For this reason, the actual inventor's skill is irrelevant: by definition, the inventor is someone with more than ordinary skill.¹⁰⁸ The person of ordinary skill is presumed to have knowledge of all pertinent prior art, the scope and content of which the factfinder has determined.¹⁰⁹ Thus, in light of the foregoing, the appropriate "question is whether what the inventor did would have been obvious to one of ordinary skill in the art attempting to solve the problem upon which the inventor was working."¹¹⁰

102. *Markman v. Westview Instruments*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc). See *Lemelson v. Gen. Mills, Inc.*, 968 F.2d 1202, 1206 (Fed. Cir. 1992), cert. denied, 113 S. Ct. 976 (1993). When the accused device is not patented, the court may construct hypothetical claims that describe the accused device. See *Wilson Sporting Goods v. David Geoffrey & Assoc.*, 904 F.2d 677 (Fed. Cir. 1990). According to this test, a court should "visualiz[e] a hypothetical patent claim, sufficient in scope to literally cover [sic] the accused product." *Id.* at 684.

103. *Markman*, 52 F.3d at 986. In determining the meaning of the claim to one skilled in the art, the court will consider the claim language, the specification, the prosecution history and extrinsic evidence, including expert testimony. *Id.* at 979.

104. See *In re Kaslow*, 707 F.2d 1366, 1374 (Fed. Cir. 1983).

105. *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934 (Fed. Cir. 1990).

106. See *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 454 (Fed. Cir. 1985). The Federal Circuit has enunciated several criteria to consider in determining the level of ordinary skill in the art. The factfinder may consider: "(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to these problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field." *Envtl. Designs v. Union Oil Co. of Cal.*, 713 F.2d 693, 696 (Fed. Cir. 1983).

107. *Standard Oil*, 774 F.2d at 454.

108. *Id.*

109. *Id.*

110. *In re Wright*, 848 F.2d 1216, 1219 (Fed. Cir. 1988) (citing *In re Rinehart*, 531 F.2d 1048, 1055 (C.C.P.A. 1976)).

It is now well settled that "[p]rior art . . . cannot be evaluated in isolation, but must be considered in the light of the secondary considerations bearing on obviousness."¹¹¹ Such evidence "may often establish that an invention appearing to have been obvious in light of the prior art was not. It is to be considered as part of all the evidence, not just when the decisionmaker remains in doubt after reviewing the art."¹¹² Examples of objective evidence of nonobviousness include commercial success,¹¹³ prior failure,¹¹⁴ unexpected results,¹¹⁵ long-felt problem or need,¹¹⁶ copying,¹¹⁷ and independent development.¹¹⁸

b. Nonobviousness and the Economic Doctrine of Equivalents

As used in the Economic Doctrine of Equivalents, obviousness is defined as the net present dollar value of investment directly related to the problem addressed by the accused device.¹¹⁹ This investment

111. *Alco Standard Corp. v. Tenn. Valley Auth.*, 808 F.2d 1490, 1499-1500 (Fed. Cir. 1986).

112. *See Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538-39 (Fed. Cir. 1983).

113. *See Akzo N.V. v. United States Int'l Trade Comm'n*, 808 F.2d 1471, 1481 (Fed. Cir. 1986) ("Commercial success is, of course, a strong factor favoring nonobviousness.").

114. *See Panduit Corp. v. Dennison Mfg. Co.*, 774 F.2d 1082, 1099 (Fed. Cir. 1985), *vacated on other grounds*, 475 U.S. 809 (1986). Prior failure to achieve the solution accomplished by the device in question may, where a sufficient showing has been made, be "virtually irrefutable evidence that . . . [the invention] would not have been obvious to those skilled in the art when it was invented." *Id. But cf. In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983) (evidence of prior failure is less persuasive where prior party had no motivation to succeed due to satisfaction with the status quo, or where prior party was unaware of the most advanced art).

115. *See Specialty Composites v. Cabot Corp.*, 845 F.2d 981, 991 (Fed. Cir. 1988) (citing *United States v. Adams*, 383 U.S. 39, 51-52 (1966)). Where an inventor proceeds "contrary to the accepted wisdom" and succeeds, there is strong evidence of nonobviousness. *In re Hedges*, 783 F.2d 1038, 1041 (Fed. Cir. 1986) (citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540 (Fed. Cir. 1983)). In another case, one expert, upon learning of the invention, found the results so unexpected that he conducted further tests over the course of three months to confirm the results. *Burlington Indus. Inc. v. Quigg*, 822 F.2d 1581, 1583 (Fed. Cir. 1987). Others skilled in the art merely dismissed the inventor as "crazy." *Id.* at 1584.

116. *See Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 935 (Fed. Cir. 1990) (nature of problem persisting in the art and the inventor's solution are factors to be considered when determining obviousness).

117. *Windsurfing Int'l, Inc. v. AMF Inc.*, 782 F.2d 995, 1000 (Fed. Cir.), *cert. denied*, 477 U.S. 905 (1986) ("Copying the claimed invention, rather than one in the public domain, is indicative of unobviousness.").

118. *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1380 n.4 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987) ("[S]imultaneous development may or may not be indicative of obviousness . . ." Moreover, as the court noted, problems regarding simultaneous development may be resolved in an interference proceeding).

119. Anyone who has enjoyed science historian James Burke's documentary series "Connections" will immediately recognize one of the problems with this definition:

represents the resources allocated to solving a particular problem. It is a monetary representation of what knowledge society would have had without the inventor's contribution. The investment used to determine obviousness is limited to that investment which has a sufficient nexus to the problem addressed by the accused device. This measurement should also be restricted to investment that occurred up to the time that the accused device was developed. These restrictions on the investment determination prevent a wealthy patentee from fraudulently and wastefully throwing money at a problem merely to increase the obviousness factor and, thereby, increase the likelihood that an accused device will infringe under the Economic Doctrine of Equivalents. Moreover, the amount of investment should not include investment by the inventor of the accused device, as it would be unfair to use an inventor's contribution against him.

This economic test of obviousness inherently includes some of the considerations of the traditional test of obviousness used to determine patentability. For example, the factfinder must determine what problem the accused device attempted to solve, i.e., what constitutes the pertinent prior art.¹²⁰ This may be done by considering investment directed to the nature of the problem confronting the inventor of the accused device, or investment in research reasonably pertinent to the particular problem with which the inventor of the accused device was involved. Furthermore, the investment included in the calculus must have a nexus to the particular problem addressed by the accused device,¹²¹ i.e., the factfinder must determine which investments contribute to the pertinent prior art.¹²² This requirement prevents the

the complex relationship of one technological development to another (and, thus, the relationship of investment in one device to the development of another). For example, Burke described how a seemingly simple development hundreds of years ago led to a chain of developments resulting in the development of the atomic bomb. *Connections* (B.B.C. T.V. & Time-Life Television broadcast, Sept. 29-Dec. 29, 1979). This problem is addressed in the Economic Doctrine of Equivalents by requiring a nexus between the investment and the problem addressed.

120. For example, suppose the accused device is a television with an improved picture tube. The pertinent art is limited to picture tube technology, not televisions generally.

121. This is analogous to the current requirement that any commercial success proffered as objective evidence of nonobviousness be a result of the merits of the claimed invention. See *Sjolund v. Musland*, 847 F.2d 1573, 1582 (Fed. Cir. 1988). Where commercial success is due to an unclaimed aspect of the invention, the factfinder cannot infer that the commercial success is due to the merits of the claimed invention. *Id.* Similarly, where investment is not directed at the specific problem addressed by the accused device, the investment cannot be included in the calculus of the Economic Doctrine of Equivalents.

consideration of investment in research that is too attenuated from addressing the particular problem.¹²³

The economic interpretation differs from the traditional nonobviousness test in that the factfinder is not required to consider a hypothetical person of ordinary skill in the pertinent art, or what would have been obvious to that person. Moreover, once the pertinent art is determined and the aggregate investment calculated, the inquiry ends. All that is relevant is the amount of investment by others in the art: the patented device is relevant only to the extent that investment in its development contributes to industrial investment in the particular problem addressed by the accused device. Under the economic test, obviousness is concerned only with the prior art. These differences greatly simplify the determination of obviousness under the Economic Doctrine of Equivalents.

2. INVESTMENT

The idea of incorporating research investment into the determination of equivalency was intimated in *Graver Tank*. After deciding that the accused composition (a flux) infringed under the doctrine of equivalents, the Court noted that, without any evidence of independent research, "the trial court could properly infer that the accused flux is the result of imitation rather than experimentation or invention."¹²⁴ Thus, the Court indicated that the absence of research investment in a device gives rise to an inference of "practicing 'a fraud on a patent.'"¹²⁵

In *Hilton Davis*, the Federal Circuit reiterated the relevance of evidence of copying.¹²⁶ The *Hilton Davis* court relied on *Graver Tank* in

122. To continue the analogy of note 121, investment is limited to development of picture tubes and picture tube technology. Thus, investment in electrical circuitry in general, for example, is too attenuated to be included.

123. For example, it is undeniable that the invention of television depended upon the successful development of electricity; however, investment in the development of electricity would not be included because that development addresses a different problem from the problems addressed by the invention of television. The point is simply this: it is not enough for a technology to be related to the accused device; rather, the technology must address the same problem as the accused device. This blatant example demonstrates that courts will have to determine what investment may be included in the obviousness calculus: this determination, far from simple addition, will require judicial interpretation as to what constitutes relevant prior art.

124. *Graver Tank*, 339 U.S. at 612.

125. *Id.* at 618. Obviously, investment would not include, in the extreme case, expenditures for industrial espionage in order to gain information as this is a blatant example of "practicing a 'fraud on a patent.'" *Id.*

126. *Hilton Davis*, 62 F.3d at 1519.

asserting that evidence of copying is relevant to a determination of equivalence.¹²⁷ However, the court expressly stated that an inference of copying "would not dominate the doctrine of equivalents analysis. Instead, where the inference arises, it must be weighed together with the other evidence relevant to the substantiality of the differences."¹²⁸

This concern with copying is addressed by the investment factor in the equation. Evidence of copying is manifested in the Economic Doctrine of Equivalents as an absence of investment. By relating investment, whether by evidence of copying or otherwise, with other factors of equivalency, the Economic Doctrine of Equivalents satisfies the Federal Circuit's concern that such evidence not dominate the analysis. Moreover, because evidence of copying may not be black or white but may be a matter of degree, using a measure of investment to represent such evidence will allow greater accuracy in attributing the proper weight to such evidence.¹²⁹ The equation requires a court to consider *any* investment directly related to the accused device. Thus, the equation facilitates consideration of research investment when such investment is readily quantifiable.

Investment should include only those expenditures that are specifically made for the accused device. For example, purchases of raw materials consumed exclusively in the production of the device are part of the investment. The entire salary of a scientist, however, could be counted toward the investment only if that scientist worked exclusively on the device; otherwise, the portion of the salary credited to investment should be prorated based on the percentage of hours that scientist worked on the device. Thus, if the scientist spent half of his time working on the device, fifty percent of his salary may be counted as part of the investment in the device.

Inadvertent invention provides an interesting illustration of the investment factor. Suppose an inventor in a microbiology laboratory creates an economically desirable strain of bacteria that is novel and nonobvious simply by accidentally leaving the cover off a petri dish. This omission allows another substance used by the scientist to react accidentally with the culture, resulting in the new bacterium. The proper consideration of investment would include overhead investment relating to the scientist's work. By contrast, suppose a person, while rummaging through his garage, accidentally knocks over a can of

127. *Id.*

128. *Id.*

129. For example, suppose an accused device comprising five components. If four of the components are copied from a patent, only the investment (if any) in developing the fifth component is included in the calculus.

something, allowing it to mix with another substance. This accident results in the invention of a commercially desirable compound that is novel and nonobvious. In this case, there is no overhead investment in the invention. This example illustrates the meaning of relevant investment in the invention. Of course, the person in the garage, after discovering the compound, could invest in developing the material. However, the length to which one must go to create a situation where the investment factor is inconsequential serves to demonstrate the relevance of this factor in the ordinary course of invention.

By considering investment, combined with commercial viability, in the determination of infringement, the Economic Doctrine of Equivalents protects accused devices which required some effort to develop and which increase efficiency. One possible criticism of this use of investment has been noted by Edmund Kitch: the patent laws should not penalize the low-cost inventor.¹³⁰ This criticism is inapposite here. Under the Economic Doctrine of Equivalents, the focus is on whether the accused device infringes the patented device, not whether or not the accused device is worthy of patent protection. Penalizing the least-cost inventor is less of a concern when the invention is accused of infringing a device which has already been deemed worthy of patent protection.

The investment factor represents competing policies: while it is true that the patent law should not penalize an inventor for developing a device with the most efficient use of resources, neither should the patent law reward an "inventor" who has simply copied other devices and made minor changes at little cost.

3. COMMERCIAL VIABILITY

Commercial viability is defined simply as the increased efficiency created by the accused device. Increased efficiency may exist in different forms, but the underlying rationale is the same: a difference¹³¹ in the accused device that results in reduction of cost. The commercial viability factor ensures that only devices that do not increase economic efficiency infringe under the Economic Doctrine of Equivalents. This is consistent with the goal of the patent system of providing incentives for inventors to provide society with beneficial products and knowledge. Although the consideration of commercial

130. Kitch, *supra* note 26, at 281. The salient distinction is that Kitch was discussing the least-cost inventor in terms of issuing a patent, rather than infringing a patent.

131. The word "difference" in this sense means one or more alterations in the accused device that preclude the literal infringement of the patentee's claims, such as an aspect of the accused device that was in the public domain.

viability in this context does not concern the patented device, it nonetheless provides the same incentive: patentees are encouraged to claim the most efficient embodiment of their inventions, thereby reducing the likelihood that an improvement on the device will have significant commercial viability. Moreover, the commercial viability factor prevents an extension of patent scope that would preclude dissemination of products and knowledge that do not infringe the literal meaning of the patent claims and increase social welfare.

The use of efficiency as an indication of commercial viability is suggested by Professors Merges and Nelson.¹³² The Economic Doctrine of Equivalents takes this use of efficiency of the accused device one step further by requiring that the increased efficiency be quantifiable as cost savings. That is, the efficiency that commercial viability represents must be a measurable reduction in cost (e.g., the cost of production or use of the claimed device). This reduction need not merely be the reduction of production costs of *making* the accused device; any difference that results in increased efficiency is relevant and therefore is included in the calculus of commercial viability.¹³³ By contrast, a mere inference that efficiency is increased by an alteration in a device would be no more helpful to the courts than the suggestion that only significant improvements in a device will not infringe under the doctrine of equivalents.¹³⁴

The Federal Circuit noted that “[e]vidence of ‘designing around’ the patent claims is also relevant to the question of infringement

132. Merges and Nelson, *supra* note 22, at 859. The authors analyze *Texas Instruments I*, 805 F.2d 1558 (Fed. Cir. 1986), and emphasize the added increased efficiency of the accused device. *Id.* at 857-59. The authors then suggest that application of the doctrine of equivalents should include consideration of “[c]hanges in the number of components; [g]reatly improved efficiency in individual components; [and i]ncreased efficiency in the way components work together, i.e., overall design components.” *Id.* at 910.

133. For example, again suppose a simple patented device of ten components. The accused device also has ten components, five of which are identical to components in the patented device and five of which are not. The accused device performs exactly the same function in exactly the same way as the patented device. The production cost of each device is the same. But the accused device performs the task in half the time taken by the patented device. If this difference manifests itself as a cost savings to the end-user, the savings represents a cost reduction, i.e., increased efficiency and thus, commercial viability.

134. For example, suppose a simple patented device comprising ten components. The accused device performs exactly the same function, in exactly the same manner, but incorporates only five components. On the surface, the accused device appears to increase efficiency. However, if the cost of making the accused device equals the cost of making the patented device (for whatever reason), then there is no increase in economic efficiency. Therefore, commercial viability is defined as increased efficiency as measured by lower cost.

under the doctrine."¹³⁵ Not only does designing around a patent require investment, but:

[t]he ability of the public successfully to design around—to use the patent disclosure to design a product or process that does not infringe, but like the claimed invention, is an improvement over the prior art—is one of the important benefits that justify awarding the patent owner exclusive rights to his invention. Designing around “is the stuff of which competition is made and is supposed to benefit the consumer.” When a competitor becomes aware of a patent, and attempts to design around its claims, the fact-finder may infer that the competitor, presumably one of skill in the art, has designed substantial changes into the new product to avoid infringement.¹³⁶

Commercial viability is a more objective, tangible measure of designing around a patent. It is a measure, not merely an inference, of competition resulting in social benefit.

Commercial viability is expressly distinguished from commercial success.¹³⁷ Professor Merges has argued that reliance on commercial success as an indication of nonobviousness in determining patentability may lead to undesirable consequences.¹³⁸ However, there may be situations where some degree of commercial success is, at least in part, indicative of commercial viability. For example, suppose a drug accused of infringement has greater efficacy than the patented drug, but has the same production cost as the patented drug. In this case, commercial success, as measured by the greater sales of the accused drug, may be the only economic measurement of commercial viability. In cases where commercial success is a proxy for commercial viability, Professor Merges' suggestion that the underlying reasons for the commercial success be considered is applicable.¹³⁹

135. *Hilton Davis Chem. Co. v. Warner-Jenkinson Co., Inc.*, 62 F.3d 1512, 1520 (Fed. Cir. 1995) (en banc).

136. *Id.* (citation omitted).

137. In part, this distinction arises from the requirement that any commercial viability, i.e., increased efficiency, arise from an improvement in the device. This excludes any cost savings from other sources, such as lower labor wages. Although production of a device by cheaper labor will result in lower cost, this is not the type of economic impact to which the Patent Act is directed.

138. Robert P. Merges, *Commercial Success and Patent Standards: Economic Perspectives on Innovation*, 76 CAL. L. REV. 803 (1988). Professor Merges argues that by blindly accepting evidence of commercial success as evidence of nonobviousness, courts run the risk of rewarding nontechnical achievements, such as superior marketing techniques, distribution systems and service networks, rather than rewarding technological invention.

139. In brief, Professor Merges recommends coupling commercial success with prior failure of others or, alternatively, scrutinizing evidence of commercial success to ensure that it is probative of invention, rather than qualities that the patent system is not designed to reward, e.g., superior advertising efforts. *Id.* at 874-75. Apparently

As a practical matter, it is worth noting that the value of commercial viability may be less than, or equal to, zero. Given the mathematical relationship, either of these situations requires judgment as a matter of law for the patentee. Where commercial viability of the accused device is nil, i.e., there is no increased efficiency resulting from the accused design, the obviousness factor will necessarily be greater and infringement can be found. Similarly, where the commercial viability of the accused device is negative, i.e., there is a decrease in efficiency resulting from the accused device, the obviousness factor will again be necessarily greater.

C. Criticisms and Strengths of the Economic Doctrine of Equivalents

Initially, it may appear that the Economic Doctrine of Equivalents incorporates criteria that examine the accused device without reference or comparison to the patented device. However, application of the Economic Doctrine of Equivalents inherently accounts for the patented device. For example, the commercial viability of an accused device must be made with reference to the patented device: an increase in efficiency will be determined by comparison to the patented device. Similarly, the obviousness factor must be calculated by including the contribution of the patented device to the prior art, to the extent that such contribution is relevant.

Strictly speaking, the Economic Doctrine of Equivalents requires a change in the traditional doctrine of equivalents paradigm which compares the accused device with the patent claims. But the new paradigm posited by the Economic Doctrine of Equivalents results from consideration of the purposes of the Patent Act and the underlying reasoning of the traditional doctrine of equivalents. This new paradigm manifests itself in an economic context. Judge Newman recognized this context by stating that "[t]he patent law is directed to the public purposes of fostering technological progress, investment in research and development, capital formation, entrepreneurship, innovation, national strength and international competitiveness. Our

courts are able to distinguish between commercial success resulting from invention and that resulting from other factors: in determining obvious *vel non* under § 103, the Federal Circuit stated that "while there is evidence that marketing and financing played a role in the success of [the patentee's invention], as they do with any product, it is clear to us on the entire record that the commercial success here was due to the merits of the claimed invention." *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1383 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987).

review of the doctrine of equivalents takes place in this context, not as an abstraction insulated from commercial reality."¹⁴⁰ Thus, the essential problem with the doctrine of equivalents is not the purpose behind the doctrine but the application of it.¹⁴¹ Failure to recognize the economic context will only result in further frustration with the doctrine.

The Economic Doctrine of Equivalents emphasizes both the prior art and the accused device. On one side of the equation, the obviousness factor is concerned with investment in the prior art. On the other side, commercial viability and investment are concerned with the accused device itself. This lesser reliance on the patented device itself decreases a court's ability to expand the claims of a patent in litigation beyond what was granted by the Patent Office.

The strength of the Economic Doctrine of Equivalents is that it focuses a court's analysis on criteria that best serve the purposes of both the Patent Act and the traditional doctrine of equivalents. First, the commercial viability factor represents the goal of the Patent Act to promote the invention, development and marketing of products that are useful to society. It thus encourages development of devices where there is no literal or fraudulent infringement and where commercial viability is great. Second, the investment factor serves to ensure that the alleged infringer does not practice a fraud on a patent. This factor also brings a tangible meaning to the notion of practicing fraud on a patent.

Some may argue that simply reducing a concept to an algebraic equation does not eliminate the uncertainty inherent in the concept of equivalence. The Economic Doctrine of Equivalents, however, reduces uncertainty as compared to the traditional doctrine of equivalents because: (1) it focuses courts on the most important considerations of the doctrine and the Patent Act; and (2) it provides a method for introducing quantitative analysis into the doctrine of equivalents. But even if the formulation provided no greater certainty than the traditional methods, it does furnish courts with a more familiar manner of analysis. This will serve to overcome any apprehension judges or juries may feel when considering highly technical matters involving infringement.

The Economic Doctrine of Equivalents may also be criticized as a simple mechanical calculation where a more flexible approach is needed. This criticism mischaracterizes the Economic Doctrine of

140. *Hilton Davis*, 62 F.3d at 1536.

141. The fact that the Federal Circuit's decision in *Hilton Davis* was 6-1-5 is justification enough for a new approach to the doctrine of equivalents.

Equivalents. The Economic Doctrine of Equivalents is an almost purely objective test; but like most rules of law, it requires some interpretation for implementation. For example, the obviousness determination requires some discretion as to whether certain investment addresses the same problem addressed by the accused device. The significant increase in objectivity achieved by the Economic Doctrine of Equivalents is not strained by the possible subjectivity of the obviousness factor. Any subjectivity introduced by the obviousness factor is more than counterbalanced by the objectivity of the overall formulation. Thus, the Economic Doctrine of Equivalents is not merely a mathematical formula applied perfunctorily by courts, but is a flexible guideline for promoting the goals of the Patent Act in accordance with the true purpose of the traditional doctrine of equivalents.

One concern raised by the use of investment in the Economic Doctrine of Equivalents is that, taken together, the investment and commercial viability factors could allow a device with little commercial viability which was backed by substantial investment to evade an infringement finding. A devious inventor could obtain insurance against an infringement finding by driving up investment in a device, irrespective of any increase in commercial viability.¹⁴² Assuming for the moment that the overinvestment is the type in which a rational investor would engage, such overinvestment does not defeat application of the Economic Doctrine of Equivalents. First, if the accused device offers no increased efficiency whatsoever, i.e., the commercial viability equals zero, then no amount of investment will avoid a finding of infringement under the Economic Doctrine of Equivalents. Second, any investment which rises to the level of fraudulence may be so identified and discounted by the factfinder.¹⁴³

The Economic Doctrine of Equivalence is also likely to be criticized for requiring quantitative analysis where it is not always possible to do so. For example, while major corporations may be able to produce the information required for the analysis, a single inventor conducting research in her garage may not be able to provide detailed information, particularly where market analysis is required. It is important to emphasize that, more than anything else, the Economic Doctrine of Equivalents is a paradigm for understanding infringement

142. It is possible to dismiss the extreme case by simply stating that rational actors would not invest in this manner. Rational actors do, however, purchase insurance, so that some overinvestment to guard against potential infringement litigation is possible.

143. For example, where an inventor purchases supplies that are readily obtained at one-third the price, the factfinder would consider only the lower price.

under the doctrine of equivalents. The Hand Formula has been subject to similar criticism. But even critics of the Hand Formula will recognize that the formula is helpful in understanding the underlying considerations of negligence. So it is with the Economic Doctrine of Equivalents. Even where a quantitative analysis is not appropriate or possible (for whatever reason), the formulation provides assistance in understanding the underlying considerations of the doctrine of equivalents and the Patent Act.

As courts¹⁴⁴ and scholars¹⁴⁵ increasingly incorporate economic analysis into legal thought and interpretation, it is not surprising that traditional legal doctrines will be revised and reformulated. Where revision and reformation through economic analysis results in a more cohesive legal doctrine, courts should not hesitate to adopt new interpretations. Given the economic nature of patent law, this particularly applies to the doctrine of equivalents.¹⁴⁶ The Economic Doctrine of Equivalents does not contravene the law as it exists: it merely serves to clarify the existing analysis in a manner more accessible to courts, inventors and investors.

V. APPLICATION OF THE ECONOMIC DOCTRINE OF EQUIVALENTS

A. Application Generally

A patentee establishes a prima facie case of infringement under the Economic Doctrine of Equivalents by introducing evidence of obviousness, investment and commercial viability which demonstrates $O > C_v \cdot I$.¹⁴⁷ Once this burden is satisfied, the alleged infringer may dispute the patentee's calculus by introducing evidence to refute the

144. See, e.g., *Carlson v. Bic Corp.*, 840 F. Supp. 457, 464 (E.D. Mich. 1993). In applying the Michigan state law of negligence, the district court noted that the risk-utility test used by the state courts is "a detailed version of Judge Learned Hand's negligence calculus"

145. See, e.g., Richard H. McAdams, *Relative Preferences*, 102 YALE L.J. 1 (1992). Professor McAdams elucidated what had confounded many adherents of economic analysis: an economic model which demonstrates the efficiency of taxation and antidiscrimination laws.

146. See generally Kenneth W. Dam, *The Economic Underpinnings of Patent Law*, 23 J. LEGAL STUD. 247 (1994); Yusing Ko, Note, *An Economic Analysis of Biotechnology Patent Protection*, 102 YALE L.J. 777 (1992); John W. Schlicher, *If Economic Welfare is the Goal, Will Economic Analysis Redefine Patent Law?*, 4 No. 6 J. PROPRIETARY RTS. 12 (1992).

147. The patentee may gain access to relevant information under the rules of discovery. Any concerns regarding confidential information may be handled by the court on a case by case basis; a court may grant a protective order to prevent dissemination of critical information.

patentee's case.¹⁴⁸ As explained below, the Economic Doctrine of Equivalents should be applied in any case where infringement is alleged, whether or not literal infringement is found.

The Economic Doctrine of Equivalents places less emphasis on the protection of pioneer inventions than the traditional doctrine.¹⁴⁹ Because a pioneer invention has virtually no prior art, the obviousness factor will be relatively small. Thus, *ceteris paribus*, infringement will be more difficult to prove in the case of a pioneer invention. This is not a fundamental flaw, however, because the Economic Doctrine of Equivalents will still function to protect only socially beneficial improvements. The purpose of the pioneer invention doctrine is to afford greater protection to those inventions that are uniquely innovative. The purpose of the Economic Doctrine of Equivalents is to protect those inventions that do not literally infringe and increase efficiency. The broad protection afforded pioneer inventions becomes unwarranted where another inventor makes an improvement, as opposed to an imitation, that is truly beneficial to society, as determined by the Economic Doctrine of Equivalents. This is especially so considering that the pioneer inventor presumably has a competitive advantage. Where the pioneer inventor has the opportunity to improve upon his own invention, but another succeeds first, the doctrine of equivalents should not protect the pioneer invention at the expense of a valuable improvement. Indeed, to do so would be contrary to the purpose of the patent law.

The advantage in applying the Economic Doctrine of Equivalents is that it inherently accounts for the uniquely innovative aspects of pioneer inventions. There is no need for a court to determine whether or not an invention should receive pioneer status. Where a pioneer invention has a greater adverse effect on the commercial viability of an accused device than a non-pioneer invention, the calculus itself will account for an invention deserving of pioneer status. Moreover, the Economic Doctrine of Equivalents does not require a court to determine whether a particular patent describes a pioneer invention; rather, by measuring a device according to its particular commercial viability, the Economic Doctrine of Equivalents recognizes that pioneer status is a matter of degree.¹⁵⁰ In cases where an accused

148. For example, the alleged infringer may challenge a portion of the amount included in the obviousness calculation as being outside the scope of the prior art.

149. See *supra* text accompanying notes 51-53.

150. This is consistent with the current application of the doctrine of equivalents to pioneer inventions: "the 'pioneer' is not a separate class of invention, carrying a unique body of law. The wide range of technological advance between pioneering

device has little or no commercial viability because the patented device is simply the most efficient embodiment of the patent, that patent will, in effect, enjoy pioneer status. But where the accused device is more efficient as a result of the defendant's effort (i.e., investment), the patented device will receive a lesser degree of protection.

In a related manner, application of the Economic Doctrine of Equivalents also accounts for the reverse doctrine of equivalents. There is no need for a court to determine whether "a device is so far changed in principle from a patented article that it performs the same or a similar function in a substantially different way"¹⁵¹ so that the reverse doctrine of equivalents applies. By applying the Economic Doctrine of Equivalents even when the accused device literally infringes the patent, the defendant has the opportunity to demonstrate, in a meaningful way, that the accused device is a substantial change from the patented device. This ensures that all the purposes of the doctrine of equivalents, in light of the goals of the patent system, are served.

B. Application to *Graver Tank*

Applying the Economic Doctrine of Equivalents to the facts in *Graver Tank* yields the same result as reached by the Supreme Court. This case also illustrates that it is unnecessary to have a strict numerical basis in order to apply the formulation. In other words, it is not necessary to know the absolute value of a factor if its relative value is known. Thus, the following interpretations of obviousness, commercial viability and investment will be made by reference to the investment in the patented device.

1. OBVIOUSNESS

Although the *Graver Tank* opinion does not provide detailed information regarding investment in the relevant prior art it is possible to draw inferences from the facts given. Certainly the investment in development of the patented composition is included in the obviousness calculus. In a case such as this, where actual figures are not available, the relative magnitude of the factor is essential.

breakthrough and modest improvement accommodates gradations in scope of equivalency. . . . The place of a particular invention in this spectrum depends on all the circumstances" *Sun Studs, Inc. v. ATA Equipment Leasing, Inc.*, 872 F.2d 978, 987 (Fed. Cir. 1989) (citation omitted).

151. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 608 (1950).

Given the insubstantial change in the accused composition, the obviousness factor in *Graver Tank* is relatively great.¹⁵²

2. COMMERCIAL VIABILITY

The facts of *Graver Tank* give rise to certain inferences that may be used to determine commercial viability. First, the fact that the accused and patented compositions were "identical in operation and produce the same kind and quality of weld"¹⁵³ suggests that the accused device did not result in anything more than a negligible increase in efficiency. Second, the similarity between the two compositions—one using silicates of calcium and magnesium, the other using silicates of calcium and manganese¹⁵⁴—gives rise to the inference that the difference in production costs of the two compositions is not great. Therefore, it is likely that commercial viability is relatively insignificant.

It is worthwhile to recognize that if the facts were such that the substitution of manganese silicates for magnesium silicates resulted in a dramatic cost savings, it is possible that there would be no infringement under the Economic Doctrine of Equivalents. Under the current doctrine of equivalents analysis, a similar noninfringement finding would be possible. Such a finding would be predicated on the substantial cost savings created by the accused device—the same criterion that the Economic Doctrine of Equivalents emphasizes.

3. INVESTMENT

Certain inferences about the degree of investment in the accused device may be drawn from the facts given. The Court noted that there was no "explanation or indication that [the accused composition] was developed by independent research . . . [and] is the result of imitation rather than experimentation or invention."¹⁵⁵ Therefore, it is apparent that investment in research of the accused composition is practically nil and, thus, relatively insignificant.

4. $O > C \vee I$

Both the commercial viability and investment factors are small; obviousness, however, is relatively great. Thus, the product of

152. The Court accepted the trial court's findings that the differences in the accused device were obvious to those skilled in the art, in light of the prior art. *Id.* at 611.

153. *Id.* at 610.

154. *Id.*

155. *Id.* at 612.

investment and commercial viability is less than the obviousness factor. Even though this may not be proven quantitatively, the facts of the case allow a court to make inferences that substantiate this conclusion. Therefore, the accused composition infringes under the Economic Doctrine of Equivalents.

VI. CONCLUSION

Arising out of the Supreme Court's admonition that "[e]quivalence, in the patent law, is not the prisoner of a formula,"¹⁵⁶ the Economic Doctrine of Equivalents provides a concise, yet comprehensive, means for applying what has proved to be a troublesome doctrine. Given all the rhetoric about protecting the virtuous inventor from the scurrilous imitator who evades infringement with minor modifications, the time has come to recognize an interpretation of the doctrine of equivalents that addresses economic impact.

The rationale behind the Economic Doctrine of Equivalents reflects the legal reasoning behind both *Graver Tank* and *Hilton Davis*. These opinions provide three fundamental principles underlying the doctrine of equivalents. First, only insubstantial, obvious changes come within the purview of the doctrine. Second, where there is evidence of copying, or conversely, no evidence of investment in the accused device, application of the doctrine of equivalents is more appropriate. Third, where there is evidence that the defendant sought to design around the patent claim, application of the doctrine of equivalents is less appropriate. These principles are adequately represented in the Economic Doctrine of Equivalents by the obviousness, investment and commercial viability factors, respectively. The relation of these factors in the equation provides a rationale for the factfinder to use in the determination of infringement under the doctrine of equivalents. Thus, the Economic Doctrine of Equivalents provides a structure for determination of infringement under the doctrine of equivalents.

Equally important is the fact that the Economic Doctrine of Equivalents uses measured quantities, not inferences, to determine equivalency. The test enunciated in *Hilton Davis* describes important considerations used to draw inferences. The test enunciated in this article describes quantification of the same considerations used to make determinations. In *Hilton Davis*, Judge Newman assessed the doctrine of equivalents:

156. *Id.* at 609.

[T]he major contribution of the doctrine of equivalents is now, and always has been, to the idea of a fairer, less technocratic, more practical patent system; one that is oriented toward encouraging technologic innovation and discouraging free riding; one that is not at the "mercy of verbalism," in the words of *Graver Tank*. In this way the doctrine of equivalents can contribute a degree of added investment confidence to the inherently risky environment of new technology. However, it will not serve that function if its application is so unpredictable that it cannot be relied upon. Indeed, the determination of technologic equivalency should be reasonably predictable by not only the innovator but also the competitor. When applied to a particular patented invention, it should be reasonably predictable whether a specific device will be found "equivalent."¹⁵⁷

Because the Economic Doctrine of Equivalents relies on measurements, rather than inferences, it is more predictable than the current test for equivalency.¹⁵⁸ The formulation provides more certainty for patent attorneys in advising their clients, as well as providing commercial actors with a legal doctrine expressed in cognizable terms. As Judge Newman concluded, "[i]t is not the doctrine of equivalents, but the uncertainty of its application, that causes the uncertainty in commercial relationships."¹⁵⁹ The Economic Doctrine of Equivalents should remove the uncertainty in the application of the doctrine.

While affording the opportunity to rein in the doctrine of equivalents, the Economic Doctrine of Equivalents remains faithful to the purposes of the traditional doctrine of equivalents, as well as the patent law in general. As Judge Newman further observed, "[n]ot all improvements are equal, and neither are their implications for technological growth."¹⁶⁰ The Economic Doctrine of Equivalents takes notice of this observation and seeks to reflect it in a manner that is consistent with the traditional doctrine of equivalents. In short, the Economic Doctrine of Equivalents provides a feasible rationale for a troublesome doctrine.

157. *Hilton Davis*, 62 F.3d at 1534 (Newman, J., concurring); see also Thomas K. Landry, *Certainty and Discretion in Patent Law: The On Sale Bar, The Doctrine of Equivalents, and Judicial Power in the Federal Circuit*, 67 S. CAL. L. REV. 1151, 1202 (1994) (concluding that "[n]o one should expect the court to achieve certainty in the doctrine of equivalents").

158. This is not to say that parties working independently of each other will arrive at the same exact measurements. Like any economic model, accuracy in the result depends on accurate information. However, the Economic Doctrine of Equivalents allows for better prediction of infringement, as well as better litigation risk assessment.

159. *Hilton Davis*, 62 F.3d at 1532 (Newman, J., concurring).

160. *Id.*

It is, perhaps, appropriate that a modification of the Hand Formula be devised to clarify and apply the doctrine of equivalents. Before the *Graver Tank* opinion issued, Judge Hand had eloquently expressed the essence of the doctrine of equivalents: "after all aids to interpretation have been exhausted, and the scope of the claims has been enlarged as far as the words can be stretched, on proper occasions courts make them cover more than their meaning will bear."¹⁶¹ The doctrine of equivalents must be preserved: it ensures that protection of an inventor's ideas is not circumvented by mere words. But equally important is the ability of inventors and investors to allocate economic resources with confidence that a court will not deprive them of the benefits of their efforts. The Economic Doctrine of Equivalents satisfies both concerns.

161. *Royal Typewriter Co. v. Remington Rand, Inc.*, 168 F.2d 691, 692 (2d Cir.), *cert. denied*, 335 U.S. 825 (1948).

COMMENT

PHYSICIANS AND SURGEONS AS INVENTORS: RECONCILING MEDICAL PROCESS PATENTS AND MEDICAL ETHICS

JOSEPH M. REISMAN[†]

TABLE OF CONTENTS

I.	INTRODUCTION	356
II.	THE CURRENT DEBATE: SHOULD MEDICAL PROCESSES BE PATENTABLE?	363
	A. The Sharing of Medical Innovations.....	368
	B. Physicians' Duties to Patients Other Than Their Own.....	370
	C. Physicians' Conflicts of Interest	370
III.	PRIOR TREATMENT OF THE ETHICAL CONSIDERATIONS RAISED BY THE PATENTING OF MEDICAL PROCESSES.....	372
IV.	HISTORICAL CONTEXT OF THE CURRENT DEBATE	376
V.	A CLASSIFICATION SCHEME FOR ADDRESSING WHETHER MEDICAL PROCESSES SHOULD BE PATENTABLE	385
	A. Medical Product Claims	386
	B. Medical "New Use" Claims	389
	C. "Pure" Medical Process Claims	391
	D. The Relevant Distinction: The Inventor's Identity.....	393
VI.	A PROPOSAL: MANDATORY ASSIGNMENT OF PHYSICIANS' PATENT RIGHTS	396
	A. Patent Clearinghouses for Physician-Invented Patents.....	397

© 1995 Joseph M. Reisman.

[†] J.D. Candidate, 1996, Boalt Hall School of Law, University of California, Berkeley; Ph.D., 1993, M.S., 1989, University of California, San Diego; B.S., 1987, Yale University. In 1996, I will serve as a judicial clerk to Judge Alan D. Lourie, United States Court of Appeals for the Federal Circuit. I wish to thank Professors Robert Merges and Marjorie Shultz for their insights and advice; Anna Jarrard, Jon Traub and William Noonan for their helpful discussions; and Gary Pulsinelli and Pilar Ossorio for their useful, thorough comments. Of course, I also thank Sara Reisman for her support and patience.

B. ASCAP as a Model for the Patent Clearinghouses.....	400
VII. CONCLUSION	402

I. INTRODUCTION

Physicians should strive continually to improve medical knowledge and skill, and should make available to their patients and colleagues the benefits of their professional attainments.

—Principles of Medical Ethics,
American Medical Association, Section 2 (1971)

The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.

—U.S. Constitution, Article I, Section 8, Clause 8

In the context of medical patents,¹ the physicians' ethical canon often conflicts with the policy goals of the federal intellectual property system. Physicians' fiduciary obligations to their patients may conflict with the "instrumental" nature of the U.S. patent system because inventors are encouraged to invest in research in hopes of later extracting profits and recovering their investments through the enforcement and licensing of the patent right.² While physicians' principal concerns must be to provide the best possible care currently available for their patients,³ the patent system encourages future

1. As used in this Comment, the term "medical patent" means a patent claiming technologies with any application to the medical treatment of humans or animals. A medical patent may contain claims for (i.e., protecting) a pharmacological composition, a mechanical device (such as a splint), a method for doing surgery, a method for using a device, a series of diagnostic steps to identify disease, or any combination of such claims. A "medical process patent" contains claims for a process (such as a surgical technique), but not claims for any distinct product. For further details of the statutory definition of patentability, see *infra* part IV and accompanying notes. See also 35 U.S.C. §§ 101-112 (1988). For a relatively brief description of the requirements of patentability, see PETER D. ROSENBERG, *PATENT LAW BASICS* chs. 6-9 (1994). For a more thorough analysis, see ROBERT P. MERGES, *PATENT LAW AND POLICY: CASES AND MATERIALS* 35-587 (1992) [hereinafter MERGES, *PATENT LAW*].

2. See generally MARC A. RODWIN, *MEDICINE, MONEY, AND MORALS: PHYSICIANS' CONFLICTS OF INTEREST* (1993); MERGES, *PATENT LAW*, *supra* note 1, at 1-10. See also E. Haavi Morreim, *Blessed be the Tie That Binds? Antitrust Perils of Physician Investment and Self-Referral*, 14 J. LEGAL MED. 359 (1993); E. Haavi Morreim, *Physician Investment and Self-Referral: A Philosophical Analysis of A Contentious Debate*, 15 J. MED. & PHIL. 425 (1990).

3. The Physician's Oath, World Medical Association Declaration of Geneva, as cited in THOMAS L. BEAUCHAMP & JAMES F. CHILDRESS, *PRINCIPLES OF BIOMEDICAL ETHICS* 441 (4th ed. 1994). See also THE HIPPOCRATIC OATH, AMERICAN MEDICAL

innovation by granting inventors the right to exclude others from practicing their innovations for a limited time.⁴ For patents containing claims⁵ for medical products (e.g., pharmaceuticals and medical devices) or medical processes (e.g., new therapeutic or surgical techniques), the operation of the patent system often means that physicians will either be barred from taking advantage of recent technological advances or, at the very least, be forced to license these advances from inventors for a fee ultimately charged to the patient.

These conflicts—between enforcing ethical norms on one hand and the policies underlying patent law on the other—have been the subject of heated debate in both the medical and legal communities for over a century,⁶ and they continue to spur controversy.⁷ This

ASSOCIATION PRINCIPLES OF MEDICAL ETHICS, and THE INTERNATIONAL CODE OF MEDICAL ETHICS, *reprinted in* ROBERT M. VEATCH, *CASE STUDIES IN MEDICAL ETHICS* 351 (1979).

4. U.S. Const. Art. I, § 8, cl. 8. Under 35 U.S.C. §§ 154, 271 (1988), a patent holder may exclude others from making, using or selling subject matter claimed in the patent for 17 years from the date of issue of a valid patent. Under recently enacted legislation to bring the U.S. into compliance with the World Trade Organization's (WTO) General Agreement on Tariffs and Trade (GATT), Pub. L. No. 103-465, patent holders may exclude others for the longer of (1) 17 years from the date of issue of a valid patent or (2) 20 years from the date of filing an application with the U.S. Patent and Trademark Office (PTO) for a patent in force or one that will issue on an application filed after on or before June 8, 1995. Patents issued on applications filed after June 8, 1995 will be enforceable for 20 years from the date of filing an application with the PTO. For further details, see *Changes to Implement 20-Year Patent Term and Provisional Applications*, 58 Fed. Reg. 63,951 (1994).

5. A patent is composed, in relevant part, of a specification and one or a series of claims. The specification "shall contain a written description of the invention, and of the manner and process of making and using it." 35 U.S.C. § 112 (1988). The claims point out with particularity the "subject matter which the applicant regards as [the] invention." *Id.* Patent claims define the "metes and bounds" of the right which the patent confers on the inventor to exclude other from making using or selling the invention and have often been compared to the limits of a real property grant. ROBERT L. HARMON, *PATENTS AND THE FEDERAL CIRCUIT* 13-15 (3rd. ed. 1994).

6. In 1855, the State Medical Society of Ohio adopted the following resolution: "[I]t is not derogatory to medical dignity, or inconsistent with medical honor, for medical gentlemen to take out a patent right for surgical or medical instruments." A national association of physicians then requested that the Ohio society either rescind that resolution or sever its affiliation with the national association. William H. Edgerton, *Medical Associations and Physicians' Patent Policies*, in *THE ENCYCLOPEDIA OF PATENT PRACTICE AND INVENTION MANAGEMENT* 563 (Robert Calvert, ed. 1964); F.E. Stewart, *Is It Ethical For Medical Men to Patent Medical Inventions?*, 29 *JAMA* 583 (1897); AMERICAN MEDICAL ASSOCIATION, *PRINCIPLES OF MEDICAL ETHICS* (1905) 12, § 8 (declaring it "derogatory to the professional character for physicians to hold patents for any surgical instrument or medicines"); Morris Fishbein, *Medical Patents*, 29 *INDUS. AND ENGINEERING CHEMISTRY* 1315 (1937).

7. See, e.g., Sabra Chartrand, *A Detection Method for Breast Tumors May Add Fire to a Debate Over Patents for Medical Procedures*, *N.Y. TIMES*, Jan. 30, 1995, at D2 (Professor Michael DeGregorio, inventor of U.S. Patent No. 5,384,260 (1995), a method of detecting breast cancer tumors that develop a resistance to Tamoxifen, expressed concern over the patenting of therapeutic methods, but was obligated to pursue the

debate has recently found its way into the United States Congress. On March 3, 1995, Representatives Greg Ganske (R-Iowa) and Ron Wyden (D-Oregon) introduced new legislation which would severely limit the patentability of medical processes, and on October 18, 1995, Senator Bill Frist (R-Tenn.) introduced legislation which would allow physicians and hospitals to infringe a class of medical patents without a license.⁸ The bills, H.R. 1127 and S. 1334 respectively, are

patent and assign the patent rights to Yale University.); Edward Felsenthal, *Medical Patents Trigger Debate Among Doctors*, WALL ST. J., Aug. 11, 1994, at B1; Luran Neergaard, *Move To Patent Surgical Procedure Sparks Fight Royalties: Doctors Say Controlling the Way They Practice Medicine in Such a Way is Unethical and Drives Up Health Care Costs*, L.A. TIMES, Apr. 2, 1995, at A14. For more scholarly analyses, see William D. Noonan, *Patenting Medical Technology*, 11 J. LEGAL MED. 263 (1990) [hereinafter Noonan, *Patenting Technology*]; William D. Noonan, *Patenting Medical and Surgical Procedures*, 77 J. PAT. & TRADEMARK OFF. SOC'Y 651 (1995) [hereinafter Noonan, *Patenting Procedures*]; and George J. Annas, *Surrogate Embryo Transfer: The Perils of Patenting*, HASTINGS CENTER REPORT, June 1984, at 25 (1984).

8. On Friday, March 3, 1995, Rep. Ganske and co-sponsor Rep. Wyden introduced the following bill and submitted it to the House Judiciary Committee:

Section 1. Short Title.

This Act may be cited as the "Medical Procedures Innovation and Affordability Act."

Section 2. Limitation On Issuance Of Patents.

On or after the date of the enactment of this Act, a patent may not be issued for any invention or discovery of a technique, method, or process for performing a surgical or medical procedure, administering a surgical or medical therapy, or making a medical diagnosis, except that if the technique, method, or process is performed by or as a necessary component of a machine, manufacture, or composition of matter or improvement thereof which is itself patentable subject matter, the patent on such machine, manufacture, or composition of matter may claim such technique, method, or process.

H.R. 1127, 104th Cong., 1st Sess. (1995).

More recently, on October 18, 1995, Sen. Frist introduced the following bill and submitted it to the Senate Judiciary Committee:

Section 1. Short Title.

This Act may be cited as the "Medical Procedures Innovation and Affordability Act."

Section 2. Noninfringing Use.

Section 271 of title 35, United States Code, is amended by adding at the end thereof the following new subsection:

"(j)(1) For any patent issued on or after the effective date of this subsection, it shall not be an act of infringement for a patient, physician, or other licensed health care practitioner, or a health care entity with which a physician or licensed health care practitioner is professionally affiliated, to use or induce others to use a patented technique, method, or process for performing a surgical or medical procedure, administering a surgical or medical therapy, or making a medical diagnosis. This section does not apply to the use of, or inducement to use, such a patented technique, method, or process by any person engaged in the commercial manufacture, sale, or offer for sale of a drug, medical device, process, or

both entitled the "Medical Procedures Innovation and Affordability Act." The House bill would make a surgical, therapeutic, or diagnostic method unpatentable unless the method involved an independently-patentable pharmaceutical composition or medical device. The Senate bill, however, would simply exempt patients, physicians and other licensed health care professionals, and health care entities from patent infringement actions if the patent claims "a drug, medical device, process, or other product that is [not] subject to regulation under the Federal Food, Drug, and Cosmetic Act or the Public Health Service Act."⁹ Because, as a practical matter, medical procedures are left unregulated by these Acts, the Senate bill would make medical process patents unenforceable against typical infringers. The American Medical Association (AMA),¹⁰ along with several other

other product that is subject to regulation under the Federal Food, Drug, and Cosmetic Act or the Public Health Service Act.

"(2) For the purposes of this subsection—

"(A) the term 'device' has the same meaning as defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 321(h));

"(B) the term 'drug' has the same meaning as defined in section 201(g) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 321(g));

"(C) the term 'health care entity' means a for-profit or nonprofit entity that provides health care services, including a hospital, medical school, health maintenance organization, group medical practice, or a medical clinic;

"(D) the term 'licensed health care practitioner' means an individual other than a physician who is licensed by a State to provide health care services;

"(E) the term 'patient' means an individual who uses a patented technique, method, or process to self-administer a medical procedure, therapy, or method of diagnosis prescribed or recommended by a physician or other licensed health care practitioner;

"(F) the term 'physician' means a doctor of medicine or osteopathy or a doctor of dental surgery or medical dentistry legally authorized to practice medicine and surgery or dentistry by a State;

"(G) the term 'product' means a machine, manufacture, or composition of matter or improvement thereof;

"(H) the term 'professionally affiliated with' includes privileges, medical staff membership, employment or contractual relationship, partnership or ownership interest, academic appointment, or other affiliation under which the physician or licensed health care practitioner provides health care services (including teaching or instructional services) on behalf of or in association with a health care entity; and

"(I) the term 'State' means any State or territory of the United States, the District of Columbia, and the Commonwealth of Puerto Rico."

S. 1334, 104th Cong., 1st Sess. (1995).

9. *Id.*

10. At Supplemental Resolution 2, A-94 (§ 480.975) (1994), the AMA condemned "the patenting of medical and surgical procedures" and announced its intention to work

medical associations,¹¹ has explicitly supported the House bill and probably will support the Senate bill as well.

It should be noted that the standard of patentability proposed in the House bill resembles the standard in the European Patent Convention, in which distinct products having medical uses (e.g., pharmaceuticals or medical devices) are patentable, but surgical or therapeutic processes are not.¹² Even though the "Medical Procedures Innovation and Affordability Act" would bring domestic patent law more closely into line with the patent laws of Europe (and, indeed, the patent laws of most other countries),¹³ neither the bills' sponsors

with Congress to outlaw the patenting of such procedures. AMA Policy Compendium Supplement, June 1994, at 30. Then, in June of 1995, Dr. John Glasson, Chair of the AMA Council on Ethical and Judicial Affairs, presented the *Report of the AMA Council on Ethical and Judicial Affairs* (June 1995) (draft on file with author) [hereinafter *AMA Report*], articulating the AMA's support for H.R. 1127 (also discussed in *AMA Criticizes Patenting of Medical Procedures*, BNA HEALTH CARE DAILY, June 21, 1995, at D5 [hereinafter *AMA Criticizes*]). See also Teresa Riordan, *Patents: New Legislation Seeks to Exclude Surgical Procedures from Patent Protection*, N.Y. TIMES, Mar. 6, 1995, at D2; Brian McCormick, *Just Reward or Just Plain Wrong?: Specter of Royalties from Method Patents Stirs Debate*, 37 AMER. MED. NEWS 33 (1994) [hereinafter *McCormick, Just Reward*]; and *Bill Would Limit Issuance of Patents on Medical Procedures*, 49 PAT. TRADEMARK & COPYRIGHT J. 530 (1995) [hereinafter *Bill Would Limit*] (general discussion of legislation).

11. Riordan, *supra* note 10, at D2.

12. The European Patent Convention provides in relevant part:

Methods of treatment of the human or animal body by surgery or therapy and diagnostic methods practiced on the human or animal body shall not be regarded as inventions which are susceptible of industrial application within the meaning of paragraph 1. This provision shall not apply to products, in particular substances or compositions, for use in any of these methods.

European Patent Convention (EPC), Article 52 ("Patentable Inventions"), ¶ 4.

In EPC Article 21(1), "inventions which are susceptible of industrial application, which are new and which involve an inventive step" are defined as patentable. The proposed U.S. legislation would differ from the EPC standard in that medical process claims would be allowable, provided a distinctly patentable composition or device was "necessary" to the method.

Under the EPC standard, no such claims are allowed. This admittedly subtle distinction is discussed in part V.C., *infra*.

13. Forty-four countries, including all members of the European Patent Convention, Japan, Canada and Mexico, exclude methods of treatment of humans and animals from patentability. GATT OR WIPO? NEW WAYS IN THE INTERNATIONAL PROTECTION OF INTELLECTUAL PROPERTY, SYMPOSIUM AT RINGBERG CASTLE, JULY 13-16, 1988, IIC Studies, Annex II, p. 299. In the December 15, 1993 General Agreement on Tariffs and Trade, Including Trade-Related Aspects of Intellectual Property Rights (GATT-TRIPS), representatives of the WTO (excluding the United States) agreed to implement uniform international standards of patentability. This particular agreement generated little controversy, for the substantive standards of patentability in the developed nations are relatively uniform with the exception of medical process patents. Article 27(3)(a) of the GATT-TRIPS agreement provides that member nations "may" exclude from patentability "diagnostic, therapeutic and surgical methods for

nor the AMA cite international harmonization as a motivating factor.¹⁴

Rather, Rep. Ganske¹⁵ believes that the new law would encourage the "sharing of medical knowledge" and would promote the traditional and more natural "evolution" of medical science. He asserts that patent protection is simply not necessary to encourage the development of innovative medical procedures because medicine develops through a process of "evolution" not "revolution."¹⁶ He also asserts that medical process patents prevent innovative surgical techniques from becoming widespread.¹⁷ For this reason, he concludes that medical process patents only serve to limit physicians' options and consequently to deny patients access to the best possible medical care.¹⁸

In part II, I review and analyze the current debate over the patenting of medical processes, paying special attention to a controversial medical process patent and its physician-inventor, Arizona ophthalmologist Dr. Samuel Pallin.

Over the last decade, several commentators have addressed the concerns raised in the current debate.¹⁹ In part III, I briefly review these analyses, focusing on the commentaries by George Annas²⁰ and Gregory Burch.²¹ I also address the more recently expressed views of Timothy McCoy²² and William Noonan.²³

the treatment of humans or animals." *Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods*, 25 INT'L REV. INDUS. PROP. & COPYRIGHT L. (IIC) 209 (1994).

14. Riordan, *supra* note 10, at D2. However, Rep. Ganske did testify before the House Judiciary Committee that more than 80 countries, including most European countries, expressly prohibit medical process patents. 1995 BNA-DAILY REPORT FOR EXECUTIVES 203 (Oct. 20, 1995).

15. Rep. Ganske is also a plastic surgeon. Neergaard, *supra* note 7, at A14.

16. *Id.*; *Patient Access to Medical Procedures Strengthened in Ganske-Wyden Bill*, U.S. Congressional News Release, Mar. 3, 1995 (on file with author) [hereinafter News Release].

17. Riordan, *supra* note 10, at D2.

18. News Release, *supra* note 16.

19. See, e.g., Timothy J. McCoy, *Biomedical Process Patents: Should They Be Restricted By Ethical Limitations?*, 13 J. LEGAL MED. 501 (1992); Noonan, *Patenting Technology*, *supra* note 7; Gregory F. Burch, Note: *Ethical Considerations in the Patenting of Medical Processes*, 65 TEX. L. REV. 1139 (1987); Annas, *supra* note 7, at 25. For a more general, and thorough, analysis of the norms of science and whether they obviate the need for intellectual property protection, see Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L. J. 177 (1987) [hereinafter Eisenberg, *Proprietary Rights*].

20. See Annas, *supra* note 7.

21. See Burch, *supra* note 19.

22. See McCoy, *supra* note 19, at 508-18.

23. Noonan, *Patenting Procedures*, *supra* note 7.

In parts IV and V, I address the special role attributed to medical processes by these commentators and by the authors of the proposed legislation. Specifically, in part IV, I present an abbreviated historical overview of the changes in patent law, medical ethics, and federal regulation of medical technology over the past century. I then use these observations to reappraise the product/process distinction currently applied to medical patents by the proposed legislation. In part V, I advance a classification scheme to analyze the ethical issues raised by the types of claims typically seen in medical patents.²⁴ This scheme separates (a) medical product claims, (b) so-called "new use" claims, and (c) "pure" surgical, therapeutic, or diagnostic procedure claims. Although these categories do overlap,²⁵ each lends itself to subtly distinct ethical and legal analyses.

I conclude that no relevant distinction, whether based on medical ethics, privacy concerns, or physicians' fiduciary duties to their patients, may be drawn among the three classes of claims for medical technologies. Instead, in subpart D of part V, I assert that the only relevant distinctions among the classes lie in who has developed the innovation and in who enforces the related patent rights.

Ultimately, I assert that only when an independent physician-inventor²⁶ pursues patent protection and then owns and enforces patent rights against other physicians are the most serious ethical concerns raised. Where an institution (bound by sufficient internal and external safeguards) pursues patent rights and sees to the licensing and enforcement of those rights, the ethical concerns raised

24. For a definition of patent claims, see *supra* note 5.

25. A single medical innovation may yield a patent containing claims from all of these classes. Moreover, if a patent discloses and claims a new medical device, the inventor is entitled to claim specific uses of and techniques for employing the device that are disclosed in the specification.

It should also be noted that patent rights for a product (e.g., a pharmacological composition or a device) necessarily include the right to exclude others from any use of that product, even if a "new" use is developed by a later innovation and is independently patentable. The holder of an earlier, broader patent may "block" the holder of a later, more narrow patent from practicing the later invention, even as the holder of the later patent may "block" the earlier inventor from practicing the more narrow invention. For a more complete discussion of "blocking" patents in the context of new uses and patentable processes, see MERGES, PATENT LAW, *supra* note 1, at 182-86.

26. I have defined "independent physician-inventors" as those who are not bound by mandatory patent assignment contracts and "institutional physician-inventors" as those bound by such agreements. While this dichotomy is by no means rigid, it provides a meaningful framework from which I will draw examples. The proposal presented in part VI provides further details regarding the independent/institutional distinctions that I find most relevant.

are far less stark. This is because institutions—unlike individuals—must constantly be willing to license technologies, and thus they are far better positioned to enforce patents without harming the rights of other physicians or patients.

In part VI, I propose a system under which individual physicians would still have powerful financial incentives to develop new and useful medical innovations, but would not themselves own or enforce the rights to the patents resulting from these innovations. The proposal, based on a suggestion made over eighty years ago, would leave intact physician-inventors' ability to patent medical processes and profit from their inventions.²⁷ Under the proposal, physicians would be bound to assign patent rights either to an approved institution or to one of several national, member-run organizations subject to the oversight of the medical community. These national organizations would act as clearinghouses for the patent rights of physician-inventors,²⁸ setting rates of compensation for inventors, issuing blanket licenses for the patent rights they own and effecting efficient yet ethical means of patent enforcement. Through this mechanism independent physician-inventors would be shielded from patent-related ethical conflicts while the competing national interests in advancing medical science and in preserving physicians' ethical conduct would be served simultaneously.

II. THE CURRENT DEBATE: SHOULD MEDICAL PROCESSES BE PATENTABLE?

The two sides of the debate over the propriety of patenting medical processes represent starkly contrasting positions. The most basic factual assumption of the proponents of patentability, that the prospect of patent protection is a necessary spur for research into better and less costly medical procedures, is flatly contradicted by the opponents of patentability.²⁹ This latter group, represented by the

²⁷. Fishbein, *supra* note 6, at 1317 (discussing proposal of 1914). The proposal is also described in the Letter of A.T. Sperry, 28 J. PAT. OFF. SOC'Y 371, 372 (1946) and in ARCHIE M. PALMER, NATIONAL RESEARCH COUNCIL, SURVEY OF UNIVERSITY PATENT POLICIES: PRELIMINARY REPORT 71 (1948).

²⁸. The similarities to copyright clearinghouses such as the American Society of Composers, Authors, and Publishers (ASCAP); Broadcast Music, Inc. (BMI); and the Harry Fox Agency may be apparent to the sophisticated reader. I discuss the similarities between the proposed medical patent rights clearinghouses and ASCAP *infra* part VI.A.

²⁹. Brian McCormick, *Restricting Patents: Bipartisan Bill Would Bar Ownership Claims for Medical Methods*, 38 AM. MED. NEWS 3 (1995) [hereinafter McCormick, *Restricting Patents*]; PTO Assails Bills to Limit Patents on Medical Procedures, 50 PATENT, TRADEMARK & COPYRIGHT J. 737 (1995).

AMA and Rep. Ganske, believe that physicians should continue to rely on traditional means for appropriating the value of their inventions, such as receiving a salary or fees that reflect their accomplishments, the acclaim of their peers ("the real glory")³⁰ and the respect of their patients. These non-patent mechanisms, it is argued, provide adequate incentives to invent new processes while maintaining the incentives to disseminate new information through the medical literature.³¹ More importantly, they argue, physicians free of the confines of the patent system would also be free to abide by their fiduciary and ethical obligations to their patients.³² Furthermore, by removing the costs of enforcing and licensing patents, either version of the proposed legislation necessarily would make medical care more affordable.³³

The position taken by the AMA and supporters of the legislation may be characterized as a narrow form of the often-expressed "Principle of Non-Removal from the Public Domain."³⁴ This underlying principle of patent law dictates that all "known" technologies should be dedicated to the public domain³⁵ and that patents should not be awarded for technologies that would have been developed without the incentives of the patent system.³⁶ Of course, it is nearly impossible to determine whether a given procedure would

30. McCormick, *Just Reward*, *supra* note 10.

31. *Hearings on H.R. 1127 and H.R. 2419 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong., 1st Sess. (1995) [hereinafter *Hearings*] (testimony of Dr. Charles Kelman, President, The American Society of Cataract and Refractive Surgery) ("[T]here is little evidence that physicians and corporate investors require [the promise of significant financial rewards] to invest in research on pure medical procedures.").

32. *Id.* (testimony of Dr. H. Dunbar Hoskins, Jr., Executive Vice President, The American Academy of Ophthalmology) (Physicians are under an ethical obligation to share "their knowledge and skills for the benefit of humanity.").

33. *Id.* (testimony of Dr. Jack A. Singer) ("A Legislative response is the only effective solution to the threat that medical method patents pose to the availability, quality, and cost of health care in our country. Failure to enact the pending legislation [H.R. 1127] will do an injustice to patients and the medical profession, while contributing to exploding health care costs.").

34. HARMON, *supra* note 5, at 11-12 ("[T]he real reason for denying patent rights is the basic principle that no patent should be granted that withdraws from the public domain technology already available to the public.").

35. See 35 U.S.C. § 102 (1988) ("Conditions for patentability; novelty and loss of right to patent").

36. See 35 U.S.C. § 103 (1988) ("Conditions for patentability; non-obvious subject matter"). See also NONOBVIOUSNESS—THE ULTIMATE CONDITION OF PATENTABILITY (J. Witherspoon ed., 1980) [hereinafter NONOBVIOUSNESS] and Robert P. Merges, *Uncertainty and the Standard of Patentability*, 7 HIGH TECH. L.J. 1 (1992) [hereinafter Merges, *Uncertainty*] (concluding that one function of § 103 is to encourage research with an uncertain prospect of success at its outset).

have been developed without the patent system when a patent system is in fact in place. Supporters of the legislation simply assert that the advances in medical science prior to the availability of medical process patents indicate that patent incentives are unnecessary, while opponents of the legislation cite the large number of applications for medical process patents as evidence, however vague, of the current need for the patent incentive.³⁷

These proponents of patentability also assert that peer acclaim is rarely based on the actual value of new inventions and, moreover, that the patent system is superior to the traditional medical literature in disseminating truly novel procedures.³⁸ Additionally, they contest any assertion that the patent system sets up perverse incentives for a physician-inventor. Instead, they claim the patent system merely creates an additional cost-benefit decision for physicians and patients who wish to license the patented process but creates no notable conflicts between the interests of physician-inventors and their own patients.³⁹ Furthermore, they note that it would be "unfair" and "counterproductive" to place physicians and surgeons, unlike all other technical professionals, outside the patent system, because the incentives of the patent system have been necessary to spur developments in the medical sciences.⁴⁰ Finally, proponents of the patent system also note that whatever conflicts of interest or additional costs are introduced by the patenting of medical

37. McCormick, *Restricting Patents*, *supra* note 29, at 3; *PTO Assails Bills to Limit Patents on Medical Procedures*, 50 PAT. TRADEMARK & COPYRIGHT J. 737 (1995). See also *Hearings*, *supra* note 31 (testimony of Dr. William D. Noonan) (noting that even though U.S. patents have been issued on surgical procedures for well over a century, the economic impact of such patents is unimportant).

38. See *Hearings*, *supra* note 31 (testimony of Michael Kirk, Executive Director, The American Intellectual Property Law Association (AIPLA)) (stating that the proposed legislation would remove inventors' incentive to develop new medical processes and to disclose newly developed techniques to the public).

39. *Id.* (testimony of Michael Kirk) (noting that conflicts only arise where a physician is "unwilling to take a license under the patent" or a patentee refuses to license his rights and further noting that "[t]he proponents of [H.R. 1127] have never been able to point to any concrete examples of patients who were at risk of not having the benefits of [Dr. Samuel Pallin's] patented surgery technique").

40. *Id.* (testimony of Donald R. Dunner, Chair, Section of Intellectual Property Law, American Bar Association):

[The Section of Intellectual Property of the American Bar Association believes] that it would be unfair to single out one area of creativity—the creation of new and improved medical procedures—and deny rewards to those creators while providing them to all others. To do so would not only be unfair, but even more importantly, would be counterproductive. Our patent system and the premises upon which it is based have been tested. That testing has gone on for more than 200 years, and has produced results which are the envy of the world.

processes, these drawbacks are dwarfed by the conflicts and escalating costs inherent in the current medical environment, which includes the uncontested presence of patents covering pharmaceuticals and medical devices.⁴¹

A single independent physician-inventor appears as a focal point for both sides in the debate: Dr. Samuel Pallin, a Sun City, Arizona, ophthalmologist. In 1990, Dr. Pallin made an upside-down V-shaped incision in a patient's eye while removing a cataract but failed to stitch the incision after surgery because the patient was experiencing heart problems. To his surprise, Dr. Pallin discovered two weeks later that the scar had healed without a suture and had far less scar tissue than a normal, sutured incision.⁴² He claims to have rushed to submit an article describing this procedure to a leading journal in the field, the *Journal of Cataract and Refractive Surgery*.⁴³ The *Journal* replied that Pallin's article offered no true innovation and summarily rejected his submission.⁴⁴

Fearing that he would never be welcome in the "good old boy network"⁴⁵ of his profession, Pallin applied for and, on January 4, 1992, received U.S. Patent No. 5,080,111: "Method of Making Self-Sealing Episcleral Incision." He then offered to donate the patent to a national cataract surgeons group, but that offer was also rejected. Finally, he offered licenses to perform the patented

41. *Id.* (testimony of Dr. William D. Noonan) (although opposed to the patenting of medical processes, Dr. Noonan testified that in spite of ethical concerns raised by pharmaceuticals and medical device patents, they were justified as incentives to invest. "The need for [patent] protection is clear with biopharmaceuticals and medical devices (or methods of using them) that may require millions of dollars for research, development, FDA approval and final marketing."). *Cf. id.* (testimony of Donald R. Dunner):

Virtually the only distinction between medical methods and medical devices is that, through the ordinary course of business, medical practitioners are insulated from direct involvement with patent-liability matters in regard to medical devices. That is, the makers of medical devices typically warrant, either expressly or by legal implication, that use of the device will not infringe another's patent right. The physician is therefore indemnified. With medical method patents, in contrast, the physician is typically the direct infringer with no indemnification. However, the mere fact that physicians are exposed to the effect of the patent laws does not suggest that those laws should be limited.

42. Jodie Snyder, *A Patent for Eye Surgery? Court Case Arises Over the Technique*, THE PHOENIX GAZETTE, Apr. 4, 1995, at A1.

43. *Id.*

44. *See Hearings, supra* note 31 (testimony of Dr. Samuel L. Pallin) ("I was denied the opportunity to publish my writings and discovery in a traditional medical journal. I turned to the U.S. Patent Office to document what I had accomplished . . .").

45. Neergaard, *supra* note 7, at A14; *see also Hearings, supra* note 31 (testimony of Dr. Samuel L. Pallin).

procedure at \$3 to \$4 per surgery, asserting that the figure was quite reasonable in light of the \$17 saved by avoiding a single suture.⁴⁶ The technique is now widely performed, although few surgeons have been willing to obtain a license from Pallin.

More insulting to Pallin, however, is the fact that Dr. Jack Singer, a Vermont ophthalmologist, claims to have invented "no-stitch" cataract surgery.⁴⁷ Singer maintains that he used a related incision a month before Pallin's discovery and that he did not seek a patent because he could not ethically seek a patent covering a medical procedure.⁴⁸ Pallin counters that his procedure is different than Singer's earlier surgery and that it yields superior results.⁴⁹ He has brought a patent infringement suit against Singer and the Dartmouth-Hitchcock Medical Center in the Federal District Court for the District of Vermont,⁵⁰ vowing that if he wins, he will charge any future licensee \$5 to use his technique.⁵¹

The debate stirred by the Pallin case has generated intense rhetoric on both sides. Pallin and his supporters note that "traditional" means of sharing medical information and technical advances failed in this case and that physicians should be encouraged to explore other means of disseminating their techniques, including filing for patents.⁵² Pallin also argues that his professional skills, which lie in inventing and developing surgical techniques, should be no less rewarded by the patent law than the professional skills of chemists and engineers, whose labors routinely yield medical patents and associated licensing fees.⁵³ In broader language, members of the legal academy have joined Pallin, noting that "[t]he whole point of the monopoly of a patent is to act as an encouragement for innovation"⁵⁴ and failing to see why physicians would respond to the

46. Neergaard, *supra* note 7, at A14.

47. Snyder, *supra* note 42, at A1; Neergaard, *supra* note 7, at A14.

48. *Hearings*, *supra* note 31 (testimony of Dr. Jack A. Singer) ("I have acted in complete compliance with the AMA code of medical ethics and the report of the AMA Council on Ethical and Judicial Affairs, which concluded: '[T]he Council believes that it is unethical for physicians to seek, secure, or enforce patents on medical procedures.'"). See also *AMA Report*, *supra* note 10 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

49. Snyder, *supra* note 42, at A1.

50. *Pallin v. Singer*, No. 593CV202 (D. Vt. filed July 6, 1993), cited in *Agency Opposes Bills to Create Patent Exception for Medical Procedures*, 1995 BNA-DAILY REPORT FOR EXECUTIVES 203 (Oct. 20, 1995).

51. Neergaard, *supra* note 7, at A14.

52. *Hearings*, *supra* note 31 (testimony of Dr. Samuel L. Pallin).

53. Neergaard, *supra* note 7, at A14.

54. Riordan, *supra* note 10, at D2 (statement of Roger E. Schechter, Professor of Law, George Washington University).

incentives of the patent system any differently than other technical professionals.

Supporters of the proposed legislation, however, see Pallin as an opportunist who seeks an endless financial reward even as he admits to expending little or no effort in developing his procedure.⁵⁵ Employing even more intense rhetoric, physicians have spoken of medical process patents as leading to the Balkanization of medicine,⁵⁶ and have compared Pallin's patent to a patent for "breaking an egg into a skillet for frying,"⁵⁷ misconstruing or simply ignoring the novelty and nonobviousness standards of patent law.⁵⁸ The AMA (perhaps playing on the public's fear of escalating medical costs) has even asserted that the cost of licensing medical process patents will add significantly to our nation's medical expenses.⁵⁹

Three central issues emerge from the current debate: (1) whether the sharing of new medical techniques is currently valued in medicine, (2) whether physicians owe duties to patients other than their own (e.g., a duty to disclose innovative techniques without seeking an economic reward) and (3) whether physician-inventors, by patenting medical processes, create conflicts between their own financial interests and the interests of their patients. Though none of these issues, strictly speaking, raises questions of patent law, understanding the manner in which each is reflected in the patent law and in medical ethics may lead to a better appreciation of the conflict and, perhaps, to a suitable resolution.

A. The Sharing of Medical Innovations

The supporters of H.R. 1127 maintain that physicians are compelled by a code of ethics to share their discoveries and knowledge with other physicians.⁶⁰ This so-called "sharing norm" may be seen in the AMA's 1971 Principles of Medical Ethics: "Physicians should strive continually to improve medical knowledge and skill, and should make available to their patients and colleagues

55. See *Hearings*, *supra* note 31 (testimony of Dr. Charles Kelman, President, The American Society of Cataract and Refractive Surgery).

56. Neergaard, *supra* note 7, at A14.

57. Editorial, *Medical Greed Patently Absurd*, DAYTON DAILY NEWS, Apr. 7, 1995, at A18.

58. 35 U.S.C. §§ 102-103 (1988) (patentable invention must be both novel and nonobvious).

59. See McCormick, *Restricting Patents*, *supra* note 29, at 3; *Bill Would Limit*, *supra* note 10, at 530.

60. "[The AMA Council on Ethical and Judicial Affairs] believes that it is unethical for physicians to patent medical procedures." *AMA Report*, *supra* note 10 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

the benefits of their professional attainments."⁶¹ Similarly, the 1991 AMA Code of Medical Ethics notes that "[t]he intentional withholding of new medical knowledge, skills, and techniques from colleagues for reason of personal gain is detrimental to the medical profession and to society and is to be condemned."⁶² Of course, the meanings of "make available" and "withhold" in these contexts are subject to a variety of interpretations, but the phrase "make available to their patients" must not mean that physician-inventors are compelled to provide their services free of charge. Likewise, is offering a license to perform a patented procedure, while simultaneously publishing results in a medical journal, a way of making that skill "available"? Although an answer to this question cannot be found in the broad language of the ethical codes, perhaps the norms of the medical community provide some guidance.

The sharing norm, in the context of "basic" (not profit-yielding) research, has been addressed in great detail by Professor Rebecca Eisenberg.⁶³ She has concluded that the perspectives of the patent system and of basic research science are often irreconcilable, and that compromises should be and have been sought to accommodate the sharing of basic research information.⁶⁴ To the extent medical research may be characterized as "basic" research, her conclusions certainly apply, but they do not to the extent that research into medical processes is "applied" (profit-yielding) research. Because medical research often defies definition as either "basic" or "applied," Professor Eisenberg's observations may not provide a great deal of guidance.

Nevertheless, her concluding observation that "the patent system will influence the behavior of research scientists more effectively if it takes into account the norms and incentives that guide behavior in the scientific community"⁶⁵ may be applied to the current debate. Only by addressing the norms of the medical community may the patent system influence the behavior of physicians and surgeons to create better incentives for innovation. For this reason, a

61. AMA PRINCIPLES OF MEDICAL ETHICS § 2 (1971), reprinted in VEATCH, *supra* note 3, at 354.

62. *New Medical Procedures*, AMA CODE OF MEDICAL ETHICS: CURRENT OPINIONS AND ANNOTATIONS 139 § 9.08 (1994).

63. Rebecca S. Eisenberg, *Patents and the Progress of Science: Exclusive Rights and Experimental Use*, 56 U. CHI. L. REV. 1017 (1989) [hereinafter Eisenberg, *Patents*]; Eisenberg, *Proprietary Rights*, *supra* note 19.

64. Eisenberg, *Patents*, *supra* note 63. (To accommodate both value systems, the author suggests that a broadened "experimental use" defense to infringement be fashioned to protect basic research.)

65. Eisenberg, *Proprietary Rights*, *supra* note 19, at 230.

compromise must be struck between the concerns expressed by physicians and by the proponents of patentability if a productive change is to be made in the patent law.

B. Physicians' Duties to Patients Other Than Their Own

The question of what duty physicians might owe to patients in general, as opposed to their own patients, is also troublesome. Under the patent law, a physician-inventor who patents a medical process is certainly free to use that technique while treating any patient,⁶⁶ but other physicians must obtain (and likely pay for) a license from the patent owner if they wish to use the patented process for their own patients. For this reason, the act of patenting a new procedure can be seen as forcing a legal relationship between the physician-inventor and other physicians' patients. A question then presents itself: What legal duties, if any, arise out of this indirect relationship?

Once again, the AMA's Principles of Medical Ethics purport to provide guidance to the individual physician:

The honored ideals of the medical profession imply that the responsibilities of the physician extend not only to the individual [patient], but also to society where these responsibilities deserve [the physician's] interest and participation in activities which have the purpose of improving both the health and the well-being of the individual and the community.⁶⁷

It appears, then, that a physician owes some duty to society at large or to the local community, but it is unclear whether that duty extends to individual members of the community. Thus, assuming a physician-inventor's duty to provide for other physicians' patients, that duty squarely contradicts the perspective of the patent system. In many ways this irreconcilable conflict parallels the conflict between the sharing norm and the patent system: physician-inventors who freely share their innovations with other physicians discharge any "responsibility" to society, but *forcing* such sharing might undermine the instrumental goals of the patent system, by eliminating the economic incentives for innovation that system seeks to create.

C. Physicians' Conflicts of Interest

An undercurrent from the much larger debate over physicians' conflicts of interest is detectable in the debate over medical process

66. Subject, of course, to Food and Drug Administration (FDA) approval of the medical devices and pharmaceuticals used in the process. See *infra* part IV.

67. AMA PRINCIPLES OF MEDICAL ETHICS § 10 (1971), reprinted in VEATCH, *supra* note 3, at 354.

patents. Conflicts of interest arise most dramatically where a physician, who owes fiduciary duties to his patients, has an economic interest that creates an incentive to act against the best interests of his patient.⁶⁸ While patent rights represent but a single means by which physicians may profit at the expense of their patients' best interests, a patient's and a physician's interests may starkly contrast in the context of patent rights.⁶⁹ For example, a surgeon may use her own patented procedure and resist using a better-suited procedure if she can avoid paying a licensing fee on the "better" alternative. A related conflict, between a physician's research directed toward a patent and a patient's right to know the physician's motives, was at issue in *Moore v. Regents of University of California*.⁷⁰

In *Moore*, plaintiff John Moore was successfully treated for hairy-cell leukemia by Dr. David Golde of the University of California at Los Angeles (UCLA) Medical Center. Golde, collaborating with other UCLA researchers, developed a valuable cell line from Moore's T-lymphocytes and obtained, for the University, a patent for the purified cell line. Neither Golde nor any of Moore's physicians disclosed the extent of the ongoing research or their developing economic interest in the outcome of that research, even as they continued to withdraw samples of Moore's "blood, blood serum, skin, bone marrow . . . and sperm" for reasons related *only* to the development of the purified cell line. The court, determining that Golde had entered into a "fiduciary"⁷¹ relationship with Moore by agreeing to treat his disease, held "a physician who is seeking a patient's consent for a medical procedure must, in order to satisfy his fiduciary duty and to obtain the patient's informed consent, disclose

68. RODWIN, *supra* note 2. The author notes: "There are two main types of conflict of interest: (1) conflicts between the physician's personal interests (often financial) and the interests of the patient and (2) conflicts that divide a physician's loyalty between two or more patients or between a patient and a third party." *Id.* at 9. The conflicts of interest that arise from physicians applying for and receiving patents are almost exclusively financial conflicts of interest. The present analysis is, accordingly, limited to financial conflicts of interest.

69. *Id.*

70. 793 P.2d 479 (1990).

71. *Id.* at 485 n.10. The court cautioned:

In some respects the term "fiduciary" is too broad. In [the context of this case] "fiduciary" signifies only that a physician must disclose all facts material to the patient's decision. A physician is not the patient's financial adviser . . . [T]he reason why a physician must disclose possible conflicts is not because he has a duty to protect his patient's financial interests, but because certain personal interests may affect professional judgment.

Id. The same limitations on the use of the term "fiduciary" should be applied to this Comment.

personal interests unrelated to the patient's health, whether research or economic, that may affect [the physician's] medical judgment."⁷²

Thus, under the *Moore* standard, potential conflicts of interest arising from physician-inventors' patents or patent applications may be largely resolved by mandating that physicians fully disclose to their patients any interests in medical patents while obtaining informed consent. Nevertheless, it is still unclear whether full disclosure would require an accounting of patent applications filed, patents held, or both. Furthermore, the developing jurisprudence of physician conflict of interest does not squarely address whether medical process patents should be granted.⁷³ Instead, it only indicates that physician-held patents create an opportunity for the interests of the physician and those of the patient to diverge. Thus, physician-held patents may be seen as creating yet another economic incentive, in a growing list, for physicians to act against the best interests of their patients.⁷⁴

Neither the rhetoric surrounding the current debate nor the underlying questions that emerge provide easy answers to our central inquiry: whether medical processes should be patentable. This uncertainty arises primarily because it is impossible to know whether patent protection is necessary to spur medical invention or whether a physician's patent rights would, even with appropriate safeguards, necessarily interfere with her duties as the fiduciary of her patients. Because of this uncertainty, the analyses of the ethical (part III) and historic (part IV) perspectives on the patenting of medical processes become crucial to understanding and reconciling the seemingly irreconcilable positions in the current debate.

III. PRIOR TREATMENT OF THE ETHICAL CONSIDERATIONS RAISED BY THE PATENTING OF MEDICAL PROCESSES

Before assessing the ethical concerns raised by the patenting of various medical technologies, it is essential to review the landscape of medical ethics and, more importantly, the recent analyses of the patent system's effect on this landscape. Several law reviews have presented articles that discuss the role of patents in medicine.

72. *Id.* at 485.

73. See RODWIN, *supra* note 2, at 212-47 (asserting that disclosure is an effective remedy for conflicts of interest, but even stricter regulatory standards for avoiding conflicts should be applied to the medical community). See also E. Haavi Morreim, *Physician Investment and Self-Referral: A Philosophical Analysis of a Contentious Debate*, 15 J. MED. & PHIL. 425 (1990).

74. See Morreim, *supra* note 73.

However, no leading text in the field of medical ethics squarely addresses the issues raised by patents claiming medical advances.⁷⁵ Nonetheless, the literature of medical ethics provides an appropriate general vocabulary for discussing the ethical concerns raised by medical patents. The terminology used by Beauchamp and Childress in *Principles of Biomedical Ethics*⁷⁶ offers a useful frame of reference by dividing the ethical landscape into five broad, overlapping categories:⁷⁷ respecting patient autonomy,⁷⁸ avoiding maleficence,⁷⁹ allowing for beneficence,⁸⁰ serving justice,⁸¹ and preserving these essential elements in the physician-patient relationship.⁸² As further analysis will reveal, patient autonomy, avoiding maleficence (in the guise of physician conflict of interest), and the physician-patient relationship are most likely to be influenced by medical patents. In addition to these concerns, medical patents may create conflicts between physicians' financial incentives and the interests of the patient,⁸³ while the enforcement of medical patents may compromise a patient's rights to privacy.⁸⁴

Recent commentaries on the patentability of medical processes have also used this framework, though each author values different ethical criteria. In *Biomedical Process Patents: Should They Be Limited By Ethical Limitations?*,⁸⁵ Timothy McCoy questions the role medical

75. See, e.g., TOM L. BEAUCHAMP & JAMES F. CHILDRESS, *PRINCIPLES OF BIOMEDICAL ETHICS* 441 (4th ed. 1994). The authors dedicate 12 pages in this 500-page treatise to "The Dual Role of Physician and Investigator," but do not discuss the patenting of an invention derived from such an investigation.

76. *Id.* See also STEPHEN G. POST, *INQUIRIES IN BIOETHICS* 1-7 (1993); VEATCH, *supra* note 3, at 59-136. Veatch, unlike Beauchamp and Childress, divides the field into four categories: duty to patient and society, health-care delivery, confidentiality, and truth-telling.

77. A recently published case book for the study of the legal issues of biomedicine has adopted this framework. See BARRY R. FURROW ET AL., *HEALTH LAW: CASES MATERIALS AND PROBLEMS* (1991). The authors dedicate entire chapters to "The Relationship of Provider and Patient" and "Access to Health Care." It should, however, be noted that this classification of ethical issues does not overlap with the classification scheme of the American College of Healthcare Executives' Code of Ethics. MARC D. HILLER, *ETHICS AND HEALTH ADMINISTRATION* 120 (1986). For further discussion of the ethical concerns that inform the decisions of health care administrators, as opposed to those of physicians, see *infra* part V.D.

78. BEAUCHAMP & CHILDRESS, *supra* note 75, at 120 (1986).

79. *Id.* at 189.

80. *Id.* at 259.

81. *Id.* at 326.

82. *Id.* at 395.

83. See generally RODWIN, *supra* note 2. See also *supra* part II.C.

84. See Jeffrey A. Taylor, Comment, *Medical Process Patents and Patient Privacy Rights*, 14 J. COMP. & INFO. L. 131 (1995).

85. McCoy, *supra* note 19.

patents play in limiting patients' access to health care⁸⁶ and information transfer,⁸⁷ while also discussing the impropriety of patenting living organisms.⁸⁸ Access to health care most directly triggers concerns for patient autonomy, justice and the physician-patient relationship. The "information-sharing ethic" cited by McCoy resembles the above-mentioned "sharing norm."⁸⁹ McCoy's third concern, whether living organisms should be patented, is generally not raised by medical process patents, and accordingly finds few parallels in the ethical scheme of Beauchamp and Childress.⁹⁰ Ultimately, McCoy concludes that the role patent protection plays in medical innovation simply outweighs any ethical concerns because patent protection creates an invaluable incentive to develop necessary medical technologies.⁹¹ In light of the heightened tenor of the current debate, however, ignoring the ethical concerns raised by the medical community may not be considered a viable option.⁹²

In *Ethical Considerations in the Patenting of Medical Processes*,⁹³ Gregory Burch discusses the controversial patent covering surrogate embryo transfer (SET)⁹⁴ (a reproductive technology that is controversial in its own right)⁹⁵ and ultimately focuses on the effect the patent might have on physician-patient relationships⁹⁶ and physician autonomy.⁹⁷ He concludes that the current patent law provides inadequate safeguards for physician autonomy and suggests that a mandatory licensing scheme for medical process patents would address this inadequacy.⁹⁸ While the approach does attempt to

86. *Id.* at 510-12, 519.

87. *Id.* at 512-14, 519.

88. *Id.* at 515-17.

89. See *infra* part II.A.

90. Cf. Robert P. Merges, *Intellectual Property in Higher Life Forms: The Patent System and Controversial Technologies*, 47 MD. L. REV. 1051 (1988) [hereinafter Merges, *Controversial Technologies*] (arguing that patent law is not the appropriate arena in which to regulate new lifeforms).

91. McCoy, *supra* note 19, at 518-19.

92. But see Noonan, *Patenting Procedures*, *supra* note 7, at 663 (noting that medical process patents have had little practical effect on domestic health care delivery and suggesting that such patents will never become more than "an occasional curiosity").

93. Burch, *supra* note 19.

94. See also Maria Bustillo et al., *Nonsurgical Ovum Transfer as a Treatment in Infertile Women: Preliminary Experience*, 251 JAMA 1171 (1984); Fern S. Chapman, *Going for Gold in the Baby Business*, FORTUNE, Sept. 17, 1984, at 41.

95. For a more thorough discussion of the ethical issues raised by SET and related technologies, see Annas, *supra* note 7, at 25.

96. Burch, *supra* note 19, at 1154-59.

97. *Id.* at 1152-54.

98. *Id.* at 1169-71.

strike a compromise, it merely forces the inevitable debate over each particular "reasonable royalty" into a court, while ignoring the United States patent law's traditional avoidance of mandatory licenses.⁹⁹

In an earlier and briefer analysis of the patenting of SET techniques, George Annas (in contrast to Burch) places a special emphasis on the invasions of patient privacy *and* on the confidential physician-patient relationship, concerns which the mere enforcement of medical process patents could compromise.¹⁰⁰ Although he admits that the prospect of patent protection was essential in generating financing for the SET research,¹⁰¹ he notes that the "subject matter" of such an advanced medical procedure "does not lend itself to patent infringement enforcement without potentially unbearable privacy violations."¹⁰² Annas then concludes that patent applications claiming these procedures should be rejected unless the applicant provides a means of enforcement that will not compromise patients' privacy rights. Jeffrey Taylor, in his Comment *Medical Process Patents and Patient Privacy Rights*, proposes just such a enforcement mechanism.¹⁰³ He suggests that Congress may revise the Patent Act to allow better access to medical records (while preserving patient privacy) during enforcement of medical process patents. For example, he suggests that removing a patient's identity from medical records subject to civil discovery in a patent infringement action would protect the patient's privacy and obviate the need for informed consent.¹⁰⁴ While this proposal might address patients' rights to privacy, it

99. In this country, only the Clean Air Act of 1970 provides for mandatory licensing of patented technology between private parties. 42 U.S.C. §§ 7401-7671 (1988). This mandatory licensing scheme, however, was only created to "curtail the tendency of patents to create a monopoly on a technology that facilitates compliance with the Act." Burch, *supra* note 19, at 1168. Furthermore, mechanisms already exist to prevent patentees from refusing to license technologies required by society. See, e.g., *Vitamin Technologists v. Wisconsin Alumni Research Foundation*, 146 F.2d 941, 944-45 (9th Cir. 1944) (*cited in* *Kearns v. Chrysler*, 32 F.3d 1541, 1551 (Fed. Cir. 1994)) (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose).

100. Annas, *supra* note 7, at 25.

101. *Id.* at 25-26.

102. *Id.* at 26. For example, Annas envisions private investigators or paid informants being used to monitor the SET process.

103. Taylor, *supra* note 84, at 147.

104. *Id.* Montana and Washington have recently enacted modified versions of the 1985 UNIFORM HEALTH-CARE INFORMATION ACT to protect the confidentiality of medical records. MONT. CODE ANN. §§ 50-16-501 to 553 (1987) (Uniform Health Care Information); WASH. REV. CODE ANN., §§ 70.02.005-904 (West 1991) (Medical Records-Health Care Information Access and Disclosure).

does not address the medical community's "sharing norm," patients' autonomy, and the potential conflicts of interest raised by physician-owned patents.

Annas' and Taylor's observations do provide an effective counterpoint to McCoy's. They assert that privacy rights simply outweigh any valid patent policy in the context of medical process patents, while McCoy asserts that the underlying policies of the patent system simply outweigh any ethical concerns. Burch, perhaps seeking a compromise, proposes a mandatory licensing scheme. But such a licensing scheme does not address Annas' assertion that enforcement of patent rights will necessarily violate patients' rights to privacy. Even if licenses were granted to all interested physicians and patients, the patent holder would be obliged to monitor operating rooms to prevent others from avoiding the (mandatory) licensing fee. It appears, then, that an alternative compromise is required to strike a meaningful balance between the principles of medical ethics and the underlying policies of the patent system.

Although each author presents compelling arguments and sound reasons to examine the ethics underlying medical process patents, each assumes that medical processes raise ethical issues distinct from those raised by medical products. Quite surprising, then, is the observation that the commentators often sweep analyses of several controversial *product* patents into their analyses of the underlying ethical questions raised by medical *process* patents. It is precisely the ease with which a discussion of medical process patents can become a discussion of medical product patents that necessitates the reassessment of ethical considerations raised by medical *process* patents, per se. In the following part, I review the major historical developments in medical ethics and patent law that have led to the controversy that today surrounds medical process patents. By tracing these developments before discussing the various ethical issues raised by each class of medical patent claims, I hope to clarify the distinctions (valid or otherwise) that have led to the current controversy.

IV. HISTORICAL CONTEXT OF THE CURRENT DEBATE

Since its inception, the U.S. patent system has served one Constitutionally mandated goal: to promote science and the useful arts.¹⁰⁵ The Patent and Trademark Office (PTO), begun as the Patent

105. U.S. CONST. art. I, § 8, cl. 8. This clause also empowers the Congress to establish a system of copyrights.

Administration under the direction of Thomas Jefferson in 1790,¹⁰⁶ has served this goal by issuing patents on worthy applications, while the federal courts have played their role by selectively enforcing or invalidating issued patents and reviewing PTO decisions.

Both the PTO and the courts, under statutes ranging from the Patent Act of 1793 (written by Jefferson) to the Revised Statutes of 1874 and the Patent Act of 1952,¹⁰⁷ have applied a "three-level" filter to distinguish inventions and discoveries worthy of patent protection from those not worthy.¹⁰⁸ To pass through the first level, the applicant must show that the claimed invention belongs among those advances that, if rewarded with a monopoly, would "promote science and the useful arts." This inquiry determines whether the application claims so-called "patentable subject matter" under 35 U.S.C. § 101 and its precursor statutes.¹⁰⁹ For example, fundamental principles, laws of nature and mathematical formulae have consistently been held not patentable subject matter because issuing monopolies for such advances might stifle scientific progress. However, mechanical devices, compositions of matter, and useful processes have, more or less consistently, been held to be patentable.¹¹⁰

Second, the applicant must demonstrate that the claimed invention is novel, that no one else has previously made the invention,¹¹¹ because rewarding a second "inventor" would not serve to promote science. Third, the applicant must show that the claimed invention is technically worthy of a patent, rather than the routine exercise of one having ordinary skill in the art. This rather ambiguous, court-made standard was long termed "the standard of invention" and was finally codified in 1952 as 35 U.S.C. § 103. It is now known as the standard of "nonobviousness."¹¹²

106. P.J. Federico, *Operation of the Patent Act of 1790*, 18 J. PAT. OFF. SOC'Y 237 (1936).

107. The current Title 35 of the U.S. Code largely resembles the Patent Act of 1952. PTO regulations may be found at 37 C.F.R. For information regarding current organization and policies of the PTO (all provided by the PTO), see "<http://www.uspto.gov>" on the World Wide Web.

108. For a more thorough description of these three "basic" standards of patentability, see MERGES, *PATENT LAW*, *supra* note 1, at 36-42.

109. Prior to the Patent Act of 1952, all the requirements of patentability were codified as § 4886 of the Revised Statutes.

110. 35 U.S.C. § 101 (1988).

111. 35 U.S.C. § 102 (1988).

112. 35 U.S.C. § 103 (1988) ("Conditions for Patentability; Non-Obvious Subject Matter"). See also NONOBLVIOUSNESS, *supra* note 36; Merges, *Uncertainty*, *supra* note 36 (concluding that one function of § 103 is to encourage research, the success of which was uncertain at its outset).

Atop this three-level filter, both the PTO and the courts have imposed barriers meant to serve more flexible ethical and public policy concerns. These concerns, though rarely raised today,¹¹³ were often manifest as a "beneficial utility" requirement.¹¹⁴ In several notable opinions ranging into the early twentieth century, the PTO and the courts denied applications for otherwise patentable devices because these devices (e.g., a coin-return device for a slot machine¹¹⁵ and a random-selecting machine for distributing toys¹¹⁶) were potentially "injurious to the morals, health, or good order of society."¹¹⁷ However, as the Food and Drug Administration (FDA)¹¹⁸ and various other administrative agencies designed to safeguard the public became more influential, the roles of the PTO and of the patent law in protecting public morals and health have diminished.¹¹⁹

An understanding of the evolving standards of patentability is essential to resolving the current debate over medical process patents. The principal argument advanced by the AMA and other proponents of the legislation is that medical processes should not pass the first filter, because granting patents for such processes—in light of physicians' ethical duties to share their innovations—is simply not necessary to spur the progress of medical science.¹²⁰ So, by granting patents for such processes, the Patent and Trademark Office (PTO) is not fulfilling its Constitutional mandate to promote science and the useful arts. The other arguments against patentability, which focus

113. In their role as courts of equity, the federal courts grant preliminary injunctions against alleged patent infringers only after considering four factors: (1) the relative rights and hardships of the parties, (2) the likelihood of ultimate success, (3) the possibility of irreparable harm, and (4) the public interest. See, e.g., *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858 (Fed. Cir.), cert. denied, 469 U.S. 856 (1984); *Datascope Corp. v. Kontron Inc.*, 786 F.2d 398 (Fed. Cir. 1986).

114. *Bedford v. Hunt*, 3 F. Cas. 37 (C.C.D. Mass. 1817). For a more general discussion, see MERGES, *PATENT LAW*, supra note 1, at 154-59.

115. *Schultz v. Holtz*, 82 F. 488 (N.D. Cal. 1897).

116. *Meyer v. Buckley Mfg. Co.*, 15 F. Supp. 640, 641 (N.D. Ill. 1936).

117. *Reliance Novelty Corp. v. Dworzek*, 80 F. 902, 904 (N.D. Cal. 1897).

118. As the proponents of S. 1334 have noted, neither the FDA nor any other government agency regulates medical procedures. See supra note 8 and accompanying discussion. A vast array of information regarding the FDA's history and current policies is available on the World Wide Web at "<http://www.fda.gov>."

119. *In re Brana*, 51 F.3d 1560, 1564 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995) and holding that the PTO may not make a prima facie finding of lack of utility for a claimed antitumor agent under the implicit utility requirement of 35 U.S.C. § 112, ¶ 1, where the applicant provides only *in vivo* murine clinical data and disapproving PTO's actions requiring explicit evidence of efficacy in human clinical trials as an encroachment on the regulatory expertise of the FDA and an unfair burden on applicants for pharmacological inventions).

120. *Hearings*, supra note 31 (testimony of Dr. Jack A. Singer).

on ethical and conflict-of-interest norms,¹²¹ though persuasive in their own right, are reminiscent of the now disfavored "beneficial utility" standard. For this reason, and because agencies other than the PTO now fulfill the role once served by the "beneficial utility" standard, these arguments against patentability should be carefully scrutinized.

The following analysis discusses the evolving standard of patentability for medical processes, the corresponding changes to the AMA's ethical code and the development of the FDA. In it, I attempt to place the current debate in context, aiding an evaluation of the various rhetorical and ethical objections to medical process patents.

While patents have been occasionally issued on medical processes since as early as 1846,¹²² the current law of medical process patents may be traced to developments in the late nineteenth century. In an 1883 decision, *Ex parte Brinkerhoff*,¹²³ the Commissioner of the Patent Office denied an application for a patent claiming a method of treating hemorrhoids.¹²⁴ The Commissioner noted that although new pharmaceutical compositions had long been considered patentable, "the methods or modes of treatment of physicians of certain diseases are not patentable."¹²⁵ The Commissioner based this conclusion on the observation that patentable discoveries, in a majority of cases, must:

accomplish certain results, but no particular method or mode of treatment under all circumstances, and in all cases will produce upon all persons the same result, and, hence to grant a patent for a particular mode of treatment would have a tendency to deceive the public by leading it to believe that the method therein described and claimed would produce the desired and claimed result in all cases.¹²⁶

In essence, the Commissioner found that medicine was neither advanced nor precise enough as a science to grant a patent in the field. The imprimatur of the PTO would unnecessarily confuse the public by suggesting that medical science was, in fact, predictable. He then held that medical processes, per se, were not patentable subject matter because of their inherent unpredictability.¹²⁷ Patents

121. See *supra* parts II.B and II.C.

122. U.S. Patent No. 4,848 (1846) (method of using inhaled ether as anesthetic).

123. 24 Comm'r Manuscript Dec. 349 (Case No. 182, July 5, 1883), reprinted in 27 J. PAT. OFF. SOC'Y. 797 (1945).

124. See I.J. Fellner, *Patentability of Therapeutic Methods*, 28 J. PAT. OFF. SOC'Y 90 (1946) [hereinafter Fellner, *Therapeutic Methods*].

125. 27 J. PAT. OFF. SOC'Y at 798.

126. *Id.*

127. *Id.*

must be reserved for only the "well-understood" arts, such as mechanics or chemistry.

At the time, such a ruling generated little controversy in the medical community. The specter of the so-called "patent medicines," typified by magical elixirs and merchants making wholly unsupported claims regarding their products,¹²⁸ loomed over the developing medical profession. This specter threatened to undermine the profession's status.¹²⁹ The medical community, in an effort to consolidate power and project a positive public image,¹³⁰ condemned any physician who "employ[ed] . . . the methods of charlatans," dealt in secret "nostrums," or merely offered "certificates attesting to the efficacy of secret medicines, or other substances used therapeutically."¹³¹ The 1905 AMA Principles of Medical Ethics also condemned the patenting of any surgical instrument or medicine by a physician as "derogatory to the professional character."¹³²

At the beginning of the twentieth century, the U.S. Congress twice (in 1902 and 1903) failed to enact legislation that would have made medical processes unpatentable.¹³³ However, by enacting the Federal Food & Drugs Act of 1906,¹³⁴ Congress did create the Food and Drug Administration (FDA).¹³⁵ Although the early FDA had little actual regulatory authority,¹³⁶ its creation signaled the eventual demise of the "beneficial utility" standard for medical patents. With the FDA's special expertise in ensuring the safety and efficacy

128. PAUL STARR, *THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE* 79-144, (1982) (chapter entitled "The Consolidation of Professional Authority, 1850-1930"). For specific examples of advertisements promoting "patent medicines," see ALBERT S. LYONS & R. JOSEPH PETRUCCELLI, *MEDICINE: AN ILLUSTRATED HISTORY* 506-07, 527, (1987) (displaying at 506-07 advertisements for, among others: "Dr. C.V. Girard's Ginger Brandy"; "No-To-Bac," a cure for nicotine addiction; and "Hood's Sarsaparilla"; and describing at 527 the success of "Dr. James's Fever Powder," a powder composed primarily of elemental antimony).

129. I leave it to the reader to decide whether confusion between "patent medicines" and "medical patents" still influences the debate over the patentability of innovations in the medical sciences.

130. STARR, *supra* note 128, at 88-92.

131. AMA PRINCIPLES OF MEDICAL ETHICS 12, §§ 7-8 (1905) ("Patents and Secret Nostrums").

132. *Id.* § 8.

133. Noonan, *Patenting Procedures*, *supra* note 7, at 654 (1995).

134. Federal Food and Drugs Act of 1906, Pub. L. No. 59-384, 34 Stat. 768 (amended 1934). See generally "<http://www.fda.gov>" on the World Wide Web.

135. For a general discussion of the role of the FDA, see Barry S. Roberts, *Regulatory Update: The FDA Speeds Up Hope for the Desperately Ill and Dying*, 27 AM. BUS. L.J. 403 (1989).

136. For example, under the Federal Food & Drugs Act of 1906, the FDA could not test medications for safety or efficacy until they had entered interstate commerce. Such delayed testing was often too late to allow the FDA to protect consumers.

of medicines, the PTO's role as guarantor of the efficacy of patented devices and processes could be, and eventually was, limited.

Into the early twentieth century, physicians continued to pursue patent protection for their innovations, despite the pronouncement of *Ex parte Brinkerhoff*, the stated policy of the AMA, and a still-ineffectual FDA. Such patents were occasionally granted, even for medical processes. In a 1930 decision, *Dick v. Lederle Antitoxin Laboratories*,¹³⁷ a district court upheld patent claims for a method of diagnosing susceptibility to scarlet fever.¹³⁸ The *Dick* court noted the diagnostic method's reproducible results and its acknowledged value in the medical community as reasons to disregard, in this case, the general prohibition of medical process patents.¹³⁹

The late 1930s marked the emergence of the FDA as a viable and effective regulatory agency. In response to the "Elixir of Sulfanilamide" tragedy of 1937,¹⁴⁰ Congress enacted the Food, Drug & Cosmetic Act of 1938.¹⁴¹ This legislation empowered the FDA to require proof of safety before approving any medication for the market, and it gave the FDA authority to enforce its decisions by inspecting and regulating interstate commerce.¹⁴² The growing power of the FDA was seen at the time as an effective complement to the PTO's regulatory efforts.¹⁴³

Soon thereafter, in the mid-1940s, a debate over the patentability of medical processes re-emerged among patent lawyers.¹⁴⁴ While a part of this debate concerned the larger issue of

137. 43 F.2d 628 (S.D.N.Y. 1930).

138. The patent in *Dick* is an excellent example of a medical patent claiming both a product and a process for using the product (the diagnostic method). Under the proposed legislation, H.R. 1127, all the claims in such a patent would be allowable, provided they met the requirements of patentability. See *supra* note 8.

139. *Dick*, 43 F.2d at 631.

140. Arthur H. Hayes, Jr., *Food and Drug Regulations After 75 Years*, 246 JAMA 1223, 1224 (1981) (discussing how, in 1937, a Tennessee manufacturer introduced a sulfa drug in liquid form which contained highly toxic diethylene glycol. The FDA conducted no safety tests prior to marketing, and at least 107 persons died after ingesting the drug).

141. 52 Stat. 1040 (1938) (currently codified at 21 U.S.C. §§ 301-392 (1994)).

142. 52 Stat. 1040, 1052, 1057. In 1976, the FDA was also empowered to regulate the sale of medical devices. However, the FDA still does not regulate the use of medical or surgical processes. CHIEF EXECUTIVE'S NATIONAL PERFORMANCE REVIEW OF THE FDA, Apr. 6, 1995, available at "<http://www.fda.gov/po/reinvent.html>" on the World Wide Web.

143. Sperry, *supra* note 27, at 371-72 (noting that the evils of "patent medicines" had been ably mitigated by the Pure Food & Drug Act and the PTO, as well as the medical profession's efforts to stigmatize medical patents).

144. Fellner, *Therapeutic Methods*, *supra* note 124. Four letters responding to the Fellner article were also published in the Journal of the Patent Office Society during 1946: Letter of George Benjamin, 28 J. PAT. OFF. SOC'Y 369; Letter of A.T. Sperry, 28 J.

whether processes, per se, should be patentable, the unique issues raised by medical processes attracted special attention. One patent attorney contended that the underlying holding of *Brinkerhoff* (that medicine was not a precise science) was untenable in the light of "modern" medical advances, and suggested that a per se rule against medical process patents delayed progress.¹⁴⁵ His arguments elicited responses not unlike those seen today. These responses ranged from the uncompromising—"[t]he sphere of medical patents does *not* include medical applications . . . This is all. This principle has to be maintained."¹⁴⁶—to the now familiar concerns for physician autonomy—"[t]he physician should be equally free to perform any therapeutic methods which his skill and education indicate."¹⁴⁷

Meanwhile, in *Martin v. Wyeth, Inc.*,¹⁴⁸ a district court withdrew from the holding in *Dick* by invalidating a claim for a method of treating mastitis in cows. The court proclaimed that medical process patents were contrary to the physicians' ethical code and thus contrary to the public interest, even as it invalidated the patent on other grounds. At about the same time, however, the AMA was reformulating its code of ethics to allow physicians more flexibility in applying for and receiving patents. The rather severe language of the 1905 Code was replaced, in 1940, by more ambiguous language: "It is unprofessional to receive remuneration from patents or copyrights on surgical instruments, appliances, medicines, foods, methods, or procedures. It is equally unprofessional by ownership or control of patents or copyrights either to retard or to inhibit research or to restrict the benefit of patients or the public . . ." ¹⁴⁹ This revised language suggests that it was acceptable for physician-inventors to patent their inventions, but not to enforce them or receive licensing fees.

In 1952, the patent law was recodified as Title 35 of the U.S. Code and the first level of the filter of patentability was codified as 35 U.S.C. § 101 ("Patentable Subject Matter"): "Whoever invents or discovers any new and useful process, machine, manufacture, or

PAT. OFF. SOC'Y 371; Letter of George Benjamin, at 28 J. PAT. OFF. SOC'Y 842; and Letter of L.A. Austrian, 28 J. PAT. OFF. SOC'Y 844. I.J. Fellner's response to the comments of George Benjamin was also published at 28 J. PAT. OFF. SOC'Y 678 (1946).

145. Fellner, *Therapeutic Methods*, *supra* note 124, at 106-08.

146. Austrian, *supra* note 144, at 844 (emphasis in original).

147. Sperry, *supra* note 27, at 371.

148. 96 F. Supp. 689, 695 (D. Md.) *aff'd*, 193 F.2d 58 (4th Cir. 1951).

149. AMA PRINCIPLES OF MEDICAL ETHICS 8, § 5 (1940) ("Patents and Perquisites"). For a revealing and extensive overview of university patent policies regarding medical patents during the 1930s and 1940s, see PALMER, *supra* note 27 (also providing synopsis of AMA ethical guidelines).

composition of matter, or any new and useful improvement thereof, may obtain a patent" For the first time the patent statute provided for the explicit protection of *processes*. In light of this new language, the PTO overruled *Brinkerhoff* only two years later in *Ex parte Scherer*,¹⁵⁰ which held that a method of jet-injecting fluids under a patient's skin was patentable. With *Scherer*, the Patent Office Board of Appeals thus formally opened the field of medical process patents. The Board effectively reversed *Brinkerhoff's* presumption that medical processes were unpredictable and hence unpatentable, noting that the new patent statute did not "categorically" define medical processes as unpatentable.¹⁵¹

In 1955, only one year after *Scherer*, the AMA again modified its view of the ethics of patenting medical devices. Now it would be ethical for a physician "to patent surgical instruments, appliances, and medicines, or copyright publications, methods, and procedures."¹⁵² Only the uses of or profits from these patents and copyrights that would "retard or inhibit research or restrict the benefits derivable" were deemed unethical.¹⁵³ The AMA condoned physicians' profiting from the enforcement of patent rights, as long as these profits did not "inhibit research" or "restrict benefits."

Recent developments have led to even broader definitions of "patentable subject matter." Hailed by many as the spark that ignited the modern biomedical industry, the Supreme Court's ruling in *Diamond v. Chakrabarty*¹⁵⁴ significantly expanded the scope of patentable subject matter by dismissing a broad range of ethical arguments designed to narrow the range of patentable inventions. In *Chakrabarty*, a narrowly divided Court held a man-made bio-organism patentable and concluded that the relevant distinction under the patent law was "not between living and non-living, but between products of nature . . . and human-made inventions."¹⁵⁵ The Court dismissed the many hazards feared to accompany biomedical science, noting that whether "claims are patentable may determine whether research efforts are accelerated by hope of reward or slowed by want

150. 103 U.S.P.Q. (BNA) 107 (Pat. Off. Bd. App. 1954).

151. *Id.* at 110.

152. AMA PRINCIPLES OF MEDICAL ETHICS 11-12, § 7 (1955) ("Patents and Copyrights"). For a review of the various AMA ethical standards during the 1950s, see Edgerton, *supra* note 6, at 564-67 (concluding that the medical profession generally endorses the use of the patent system as a tool for bringing inventions into general use, provided the invention is made widely available and is exploited with dignity).

153. AMA PRINCIPLES OF MEDICAL ETHICS 11-12, § 7 (1955) ("Patents and Copyrights").

154. 447 U.S. 303 (1980) (Burger, J.) (5-4 decision).

155. *Id.* at 313.

of incentive,"¹⁵⁶ but need not determine the ultimate value of the research to society. Other regulatory agencies, such as the FDA, could better determine the social and medical value of such inventions.¹⁵⁷ The Court intimated that if Congress felt a need to monitor an ethically troubling technology, it could empower an agency to oversee that technology.¹⁵⁸ The same reasoning may be at work in the current Senate bill.¹⁵⁹ That bill would apparently provide that if and when FDA authority expands to govern medical processes, medical process patents would be enforceable against physicians, patients, or other health care entities. However, as long as no federal agency is empowered to regulate the use of medical processes, medical process patents should be, by and large, unenforceable.

The creation of the Court of Appeals for the Federal Circuit (CAFC) in 1982¹⁶⁰ further signaled a strengthening of the patent grant, as it unified the appellate jurisdiction of patent disputes and judicial review of the PTO in a single federal appellate court. The CAFC recently sealed the fate of the "beneficial utility" standard for medical patents. In *In re Brana*, the court (with the PTO's blessing) yielded all authority to regulate the safety and efficacy of medical products to the FDA.¹⁶¹ If and when the scope of federal regulatory authority expands to govern the use of medical processes, *Brana* suggests that the PTO would again yield to a sister agency.

In light of the broad construction of 35 U.S.C. § 101 now favored by the courts, the unified jurisprudence of the CAFC, and the ever-relaxing ethical standards of the AMA, it should come as no surprise that medical process patents have become quite

156. *Id.* at 317.

157. *Id.*

158. *Id.*

159. See *supra* note 8 and accompanying text.

160. The Federal Courts Improvement Act of 1982, Pub. L. 97-164, 96 Stat. 25 (codified, in part, as 28 U.S.C. § 1295(a) (1988)) (including in the jurisdiction of the CAFC appeals from decisions of the PTO Board of Patent Appeals and Interferences and of federal district courts to which a case was directed pursuant to Title 35 of the U.S. Code (The Patent Act)).

161. 51 F.3d 1560, 1567 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995)). See also "<http://www.fda.gov/opacom/hpcdrh.html>" (describing the FDA's Center for Devices and Radiological Health, which is responsible for ensuring the safety and effectiveness of medical devices), "<http://www.fda.gov/opacom/hpdrug.html>" (describing the FDA's Center for Drug Evaluation and Research, which regulates prescription and over-the-counter medicines for human use), and "<http://www.fda.gov/opacom/hpvet.html>" (describing the FDA's Center for Veterinary Medicine, which ensures that animal drugs and medicated feeds are safe and effective), all on the World Wide Web.

commonplace.¹⁶² Nonetheless, in a June 1994 resolution, the AMA condemned physicians who would seek patents for "medical and surgical" procedures,¹⁶³ while it continued to tacitly approve physicians who would patent surgical or diagnostic instruments.¹⁶⁴

In view of the medical community's continually changing views on the ethics of obtaining medical patents,¹⁶⁵ as well as the changing role of the PTO in adjudicating the social and ethical worth of patent applications, the AMA's support of the pending legislation¹⁶⁶ should raise some eyebrows at the very least. In the following part, I advance a scheme better suited to understanding the implications medical patents have for the ethical concerns of patient autonomy and privacy, as well as for physicians' potential conflicts of interest. Using this scheme as a framework, I then propose a mandatory assignment system for physician-inventors, which will address both the concerns of the medical community and the underlying policies of the patent law.

V. A CLASSIFICATION SCHEME FOR ADDRESSING WHETHER MEDICAL PROCESSES SHOULD BE PATENTABLE

The foregoing analysis suggests that the proposed statutory distinctions between medical product claims and medical process claims may be no more than historical accident. However, the historical analysis alone does not address the possibility that serious ethical and practical differences may be reflected in the distinction between medical products and processes sought in the proposed legislation. In this part, I address the ethical and social concerns

162. See Noonan, *Patenting Procedures*, *supra* note 7, at 658-60 (1995) (Table 1, listing 48 selected medical process patents but maintaining that such patents are not a "recent phenomenon"). See also Felsenthal, *supra* note 7, at B1; Neergaard, *supra* note 7, at A14.

163. At Supplemental Resolution 2, A-94 (§ 480.975) (1994) the AMA condemned "the patenting of medical and surgical procedures" and announced its intention to work with Congress to outlaw the patenting of such procedures.

164. AMA CODE OF MEDICAL ETHICS: CURRENT OPINIONS AND ANNOTATIONS 140, § 9.09 (1994) ("Patent for Surgical or Diagnostic Instrument"), which provides: "A physician may patent a surgical or diagnostic instrument he or she has discovered or developed. The laws governing patents are based on the sound doctrine that one is entitled to protect one's discovery."

165. I am aware that the AMA does not represent the entire medical community. I have simply chosen the AMA as a convenient mechanism to trace the evolving views of the medical community.

166. In June of 1995, Dr. John Glasson, Chair of the AMA Council on Ethical and Judicial Affairs, presented the *AMA Report*, *supra* note 10, articulating the AMA's support for H.R. 1127 (also discussed in *AMA Criticizes*, *supra* note 10, at D5).

raised by the three broad classes of medical patents and focus on the three chief ethical concerns discussed in part III: autonomy of patients and physicians, patients' rights to privacy, and the maintenance of sound physician-patient relationships. I then conclude that while the two pending bills crudely distinguish among types of medical patents, neither resolves the ethical concerns common to the classes. Rather, a distinction based on whether or not a physician owns the patent would more effectively address the ethical concerns raised by medical patents.

A. Medical Product Claims

The first class of patent claims, those protecting new medical products (and necessarily protecting their use in medical treatments), are typified by claims for synthetic drugs and medical devices.¹⁶⁷ Such innovations are patentable in the U.S.,¹⁶⁸ throughout Europe,¹⁶⁹ and, under the recent General Agreement on Tariffs and Trade, Agreement on Trade Related Aspects of Intellectual Property Rights (GATT-TRIPS) accord, in all World Trade Organization (WTO) countries.¹⁷⁰ It is thus accurate to say that international consensus supports the patentability of medical products.

This consensus seems odd, however, in view of the developing international controversy surrounding the patenting and marketing of pharmaceuticals.¹⁷¹ For example, Glaxo PLC, the world's second largest pharmaceutical producer and owner of a patent for the best-selling prescription medicine Zantac, has recently seen its sales decline as entire countries,¹⁷² as well as several domestic health

167. Medical product claims are often classified by the PTO as belonging to either utility patent class 424 ("organic compounds/medical") or classes 602-604 ("Medical & Surgical Equipment").

168. 35 U.S.C. § 101 (1988) ("any new and useful process, machine, manufacture, or composition of matter" is patentable).

169. EPC Article 52(4). See *supra* note 12.

170. General Agreement on Tariffs and Trade, Agreement on Trade Related Aspects of Intellectual Property Rights (GATT-TRIPS) Article 27 ("Patentable Subject Matter") provides, in part: "[§ 1] [P]atents shall be available for any invention, whether products or processes, in all fields of technology, provided they are new, [are non-obvious] and are capable of an industrial application," subject to the provision that member states may exclude from patentability "[§ 3(a)] diagnostic, therapeutic and surgical methods for the treatment of humans or animals."

171. See, e.g., Stephen D. Moore & Elyse Tanouye, *Innovation Fails to Shield Glaxo in HMO World*, WALL ST. J., Jan. 25, 1995, at B1, B4.

172. *Id.* at B4 ("[T]he French government has refused to pay for patients' use of the [highly-touted migraine] drug, as it is still wrangling with Glaxo over a price, and health authorities in the Netherlands wrested sizable price cuts by threatening to deny coverage for its citizens.").

maintenance organizations (HMOs), have refused to purchase particular pharmaceuticals. These countries and HMOs believe the drug is overpriced and redundant of less expensive options.¹⁷³ While these developments may be seen as mere market corrections for overpriced goods, the fact remains that millions of patients are denied access to such new treatments by the elevated prices often attached to patented pharmaceuticals,¹⁷⁴ as well as by governmental and HMO austerity measures.

Even more severe ethical objections are raised where a patent holder exercises its right to exclude others from the market while not producing the patented medical product itself. Although every medical product claim potentially raises this concern, the courts do consider the potential public harm of enforcing an injunction in favor of such an unscrupulous patentee.¹⁷⁵ For example, in *Milwaukee v. Activated Sludge, Inc.*,¹⁷⁶ the appellate court denied an injunction against the use of a waste treatment system on the theory that enforcement would have created an irreparable harm to the local community.¹⁷⁷ The CAFC has suggested¹⁷⁸ that it will continue to deny injunctions where the patent-holder has simply failed to exploit its

173. *Id.*, at B1, B4.

174. The patent grant gives its owner the right to prevent others from selling the patented product during the patent term. If the patentee can sell the product during that term and no noninfringing substitute is available to consumers, the patentee can elevate the price of the product without fear of direct competition in a narrowly defined market. The potential to capture such a market, in essence, creates the incentives underlying the patent system. For a more detailed analysis of these incentives, see Eisenberg, *Patents, supra* note 63, at 1024-30.

175. 35 U.S.C. § 283 (1988) provides that federal courts have jurisdiction to "grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent, on such terms as the court deems reasonable." The CAFC has justified always considering public benefits and harms when reviewing injunctions by noting that the standards of public interest, not the requirements of private litigation, measure the need for injunctive relief, *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858, 868 (Fed. Cir.), *cert. denied*, 469 U.S. 856, 865-66 (1984), and that "[i]f Congress wants the federal courts to issue injunctions without regard to historic equity principles, it is going to have to say so in explicit and even shameless language," *id.* at 867 (quoting *Hecht Co. v. Boules*, 321 U.S. 321, 331 (1944)). See also *Reebok Int'l v. J. Baker, Inc.*, 32 F.3d 1552, 1555 (Fed. Cir. 1994); *Chrysler Motors Corp. v. Auto Body Panels of Ohio*, 908 F.2d 951, 954 (Fed. Cir. 1990).

176. 69 F.2d 577 (7th Cir.), *cert. denied*, 293 U.S. 576 (1934).

177. *Id.* at 593.

178. In *Kearns v. Chrysler*, 32 F.3d 1541, 1551 (Fed. Cir. 1994), the court cited *Vitamin Technologists v. Wisconsin Alumni Research Foundation*, 146 F.2d 941, 944-45 (9th Cir. 1944) (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose). The court used this citation to support the uncontroversial proposition that "the right to exclude . . . is not absolute even during the life of a patent, but is discretionary." *Kearns*, 32 F.3d at 1551.

patent rights,¹⁷⁹ or when an injunction would deny the public access to necessary medical products.¹⁸⁰ Nevertheless, the owner of a vital medical product patent may lawfully extract monopoly prices during the term of the patent and thus can create severe barriers to most patients' access to health care.

The enforcement of surgical device patents, covering either devices used during surgery or those left in the body of the patient, may also infringe upon patients' rights to privacy.¹⁸¹ Where a claim protects a device, a patent owner need only "mark" the device with the U.S. patent number to assure the recovery of damages¹⁸² from anyone who "uses or sells" the device without the permission of the patent owner.¹⁸³ In *American Medical Systems, Inc. v. Medical Engineering Corp.*, the CAFC justified this rule in the context of claims covering an implanted medical device and a method of implanting the device.¹⁸⁴ The court's ruling suggests that both physicians (by using or selling medical devices) and patients (by using medical devices) may be liable for damages, even where an implanted, hence unseen, device is used. To enforce such claims, a patentee (or, perhaps, a court) may be forced to inspect whether an appropriate "mark" was affixed to the implanted device, potentially encroaching upon patients' rights to privacy during and after surgery.

Agreements between physicians and pharmaceutical or medical device companies may also lead to severe conflicts between the financial interests of the physician and those of the patient. For example, if a physician were compensated by a patentee for

179. *E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 835 F.2d 277 (Fed. Cir. 1987) (denying injunction).

180. *Vitamin Technologists*, 146 F.2d at 945 (denying injunction where patentee refused to license its process for producing vitamin D to those who would fortify oleomargarine and infringer used process for that purpose).

181. *Annas*, *supra* note 7, at 25.

182. 35 U.S.C. § 287(a) (1988). *See also* *American Medical Sys. v. Medical Eng'g Corp.*, 6 F.3d 1523, 1538 (Fed. Cir. 1993), holding:

The purpose behind the marking statute is to encourage the patentee to give notice to the public of the patent. The reason that the marking statute does not apply to the method claims is that, ordinarily, where the patent claims are directed to only a method or process there is nothing to mark. Where the patent contains both apparatus and method claims, however, to the extent that there is a tangible item to mark [the patent holder must affix a mark to] avail itself of the constructive notice provisions of section 287(a).

183. 35 U.S.C. § 271(a) (1988).

184. *American Medical Sys.*, 6 F.3d at 1538-39 (holding claims for an inflatable, prosthetic penile implant and for a method for implanting the device were infringed willfully, but where no notice of a valid U.S. patent appeared on the device, district court correctly denied damages).

prescribing a patented medication, the physician would have strong financial interests potentially adverse to the interests of the patient. Only in extreme cases does medical malpractice liability provide incentives counter to the positive incentives for financial agreements between physicians and pharmaceutical companies. Where several courses of treatment are available, the potential for abuse and conflicts of interest should be self-evident. In fact, the regulation of agreements between pharmaceutical manufacturers and physicians is currently the subject of intense debate,¹⁸⁵ indicating that the more narrow concerns raised by medical product patents are real.

In light of these strong ethical and conflict-of-interest concerns, the consensus of support for medical product patents may seem odd. However, when the high costs of developing new and more effective pharmaceuticals and the strong regulatory role entrusted to the FDA are considered,¹⁸⁶ rationales for protecting medical product claims do emerge. The investments needed for research expenditures justify patent protection; and, because most product patent owners are not physicians and may be prevented from influencing physicians, situations that give rise to conflicts of interest may be avoided through appropriate regulation. These considerations soften the ethical and conflict-of-interest concerns of medical product patents, if only slightly.

B. Medical "New Use" Claims

The second class of patent claims, those protecting new medical uses for known products, presents a distinct set of ethical dilemmas because the product is "available" but the use valued by physicians and their patents is protected by a distinct claim. This class of claims is typified by any newly discovered medical applications of a known technology,¹⁸⁷ such as the use of a laser in arterial surgery¹⁸⁸ or the use of a hair loss treatment to combat a reproductive disorder.¹⁸⁹

185. RODWIN, *supra* note 2, at 55-94.

186. The FDA is empowered to regulate pharmaceuticals for human or animal use, medicinal feeds for animals, and medical devices. For more information, see generally "<http://www.fda.gov>" on the World Wide Web.

187. Medical "new use" claims, like medical product claims, are often classified by the PTO as belonging to either class 424 ("organic compounds/medical") or classes 602-604 ("Medical & Surgical Equipment").

188. See U.S. Patent No. 4,862,886 (1989) ("Laser Angioplasty"). Assignee Summit Technologies owns eight patents related to the use of lasers in medical treatments. While some of these patents are, strictly speaking, medical process patents, many contain specific "new use" claims for the purposes of this analysis.

189. See U.S. Patent No. 5,336,678 (1994) ("Use of Minoxidil for Treating Erectile Impotence").

Under the House bill these claims would not be allowable unless the underlying technology, be it a device or a pharmaceutical, is independently patentable.¹⁹⁰ However, under the Senate bill these claims would be allowable and could be enforced against physicians if the "known" technology were a drug or device subject to either the Food, Drug and Cosmetics Act or the Public Health Service Act.¹⁹¹ The House bill would effectively eliminate medical "new use" claims, while allowing owners of product patents, alone, to license *all* uses of their product, even those uses developed by others.¹⁹²

This proposed elimination of medical "new use" claims is startling, because the strong ethical objections raised against medical product patents are often tempered by the existence of other patents containing "new use" claims. In the context of a "new use" patent "blocked" by an earlier product patent, *neither* patent owner may lawfully practice the invention without a license from the other. In such a situation, both patentees must compromise to bring the product to market and, often, artificially elevated prices cannot be maintained because both patentees ultimately enter the market.¹⁹³ Where no "new use" claims may be granted, the original patentee may forbid any use of the product and may extract monopoly prices for whatever new medical uses it, or others, develops. This perverse situation creates strong *disincentives* for the development (and disclosure) of new medical uses of a patented product by anyone other than the original patentee, since all financial benefits derived from the new use would return to the original patentee instead of being shared by both inventors.¹⁹⁴

Despite this odd consequence, the elimination of "new use" claims does alleviate certain ethical objections, especially the objection that "new use" claims potentially inhibit physicians' autonomy. Traditionally, physicians have had broad authority to prescribe any FDA-approved pharmaceutical for any ailment, even if

190. See H.R. 1127, *supra* note 8.

191. See S. 1334, *supra* note 8.

192. *Hearings, supra* note 31 (testimony of Dr. Frank Baldino, Jr., President and Chief Executive Office of Cephalon, Inc.). Dr. Baldino testified that "despite the voiced intention of only focusing on pure medical procedure patents, H.R. 1127 would prevent the issuance of precisely the types of patents [new use patents] which Cephalon and members of our industry must secure in order to protect our discoveries."

193. MERGES, PATENT LAW, *supra* note 1, at 182-86.

194. Admittedly, the term of the original product patent and that of the "new use" patent may overlap for only a few years. In such a situation, the "new use" would enter the public domain more rapidly under H.R. 1127 than it does under the present system, but the strong disincentives for anyone but the patentee developing a medical "new use" during the term of the product patent would still remain.

the compound is not suggested for the prescribed use. "New use" claims, if enforced, would limit a physician's ability to prescribe useful drugs as freely as the traditional principles of physician autonomy suggest.

The elimination of "new use" claims might also allay some concerns regarding physicians' conflicts of interest. Physician-inventors with patent rights for new medical uses might encourage other physicians to use or license these uses, even though cheaper or more effective treatments are available. By eliminating "new use" claims, the House bill removes this potential conflict of interest in much the same way it eliminates the potential conflicts that arise from medical product claims. However, even if the elimination of "new use" claims would allay present concerns over physicians' autonomy and potential conflicts of interest, it would do so while creating a perverse incentive against developing new medical uses for already patented products and a concurrent incentive to conceal all such developments during the term of the dominant product patent. With regard to "new use" patents, then, the Senate bill may be a viable alternative since it would retain "new use" patents and leave the vast majority of such patents enforceable.

C. "Pure" Medical Process Claims

The third and final class of medical claims, those protecting only manipulative steps such as surgical procedures, would be unpatentable under the House bill and unenforceable under the Senate bill.¹⁹⁵ The patenting of medical and surgical techniques triggers concerns over both the "sharing norm" in the medical community and the invasion of patients' rights to privacy. However, the specter of physician-inventors enforcing their patent rights by sending investigators into operating rooms to oversee potentially infringing procedures most directly triggers concern only over patients' rights to privacy.¹⁹⁶

The mechanics of enforcing patent rights is also important in that it blurs the distinction between the scope of patent protection available under the European Patent Convention (EPC), Article 52, and that available under the proposed legislation. The EPC makes all medical processes unpatentable, but it allows for the patenting of medical devices.¹⁹⁷ The House bill is distinguishable in that it would allow for a patent covering a medical process, provided that an

195. S. 1334, *supra* note 8.

196. Annas, *supra* note 7, at 25-26.

197. EPC Art. 52 ("Patentable Inventions"), ¶ 4. See *supra* note 12.

independently patentable device is "necessary" to the process."¹⁹⁸ In the context of enforcement (where the real-world value of the patent right is determined), this subtle distinction becomes irrelevant. Enforcement of patent rights will rely on detection of the underlying device under either regime. Under the House bill, the process patent could not exist, and would therefore have no value, without the claim covering the "necessary" device. Thus, the narrow exception of the House bill becomes all but meaningless.

The Senate bill takes a different approach. Under it, most "pure" medical or surgical processes would be patentable but would not be enforceable. To differentiate between patents protecting "pure" processes and the two other types of medical patents, the bill relies on the limited regulatory authority of the FDA.¹⁹⁹ As noted above, the FDA has the authority to regulate medical devices and pharmaceuticals but no direct authority to regulate medical or surgical procedures. Because procedure patents (unlike the two other types of medical patents) are not the subject of federal regulation, only patents for "pure" medical procedures would be unenforceable under the Senate bill.

Nevertheless, both bills address some of the potential conflicts of interests that may arise for physicians who own patent rights for new processes. Incentives presently exist, and would still exist under the narrow exception of the House bill, for a physician-inventor to recommend to other physicians, as well as to his patients, that they practice his patented surgeries. These conflicts are especially acute because of physicians' special roles as medical advisors. Relatively free of FDA regulation when prescribing "pure" surgical or diagnostic procedures, physicians (especially surgeons) are entrusted with critical surgical decisions by many patients, even though they are also the very individuals who patent, and profit from, these recommended surgical procedures.

The Senate bill addresses this conflict by tying enforceability to the scope of FDA regulatory authority. But concerns about patients' rights to privacy and physicians' conflicts of interest would not disappear if the FDA (or another federal agency) were given the authority to regulate medical or surgical procedures. Furthermore, the Senate bill fails to address the many ethical concerns raised by physician-owned patents other than the narrow class of "pure" process patents.²⁰⁰ The bill may also create an artificial reason to limit the

198. H.R. 1127, *supra* note 8.

199. S. 1334, *supra* note 8.

200. See generally Noonan, *Patenting Procedures*, *supra* note 7.

scope of FDA authority so that medical process patents would be enforced. Therefore, although the Senate bill may be a superior alternative since it addresses a concern the House bill does not, it fails to identify the only truly relevant distinction among the three types of medical patents.

D. The Relevant Distinction: The Inventor's Identity

The foregoing analysis of the three classes of medical patent claims indicates that, from the narrow perspective of medical ethics, the classes are not distinguishable in any meaningful way. While medical "new use" and process claims may lead to conflicts of interest more difficult to regulate than those of medical product claims, medical product claims present stark ethical dilemmas by restricting physician autonomy, patient autonomy, and access to health care. Also, medical product claims, if strictly enforced, threaten patients' rights to privacy far more severely than either "new use" or process claims.

The PTO and the courts might also find it difficult to distinguish "mere" medical process claims from otherwise patentable claims under the House bill and, likewise, to determine the precise scope of FDA authority under the Senate bill. The courts that interpret the EPC (where therapeutic methods are not patentable but industrial applications are)²⁰¹ have struggled with this distinction. These struggles should caution against the use of rules that draw facile distinctions between "medical" innovations, which are to be freely shared, and "industrial" innovations, which might be kept secret if not for the prospect of patent protection. The European Patent Organization's Technical Board of Appeal, in *In re Bayer AG*,²⁰² was forced to decide if the addition of a particularly effective immunostimulant to poultry feed for boosting market weight was an unpatentable "method of treatment of the animal body" or a patentable process "susceptible to industrial application." The Board based its holding of unpatentability on rather opaque reasoning: (1) the medical aspects of the process were "inextricably linked to" rather than "distinct from" the cosmetic aspects,²⁰³ (2) the process was "curative" rather than "prophylactic,"²⁰⁴ and (3) increased market

201. EPC Art. 52 ("Patentable Inventions"), ¶ 4. See *supra* note 12.

202. Decision of the Technical Board of Appeal 3.3.2, T780/89 (Aug. 12, 1991), OJ EPO 7/1993, 440. It is unclear whether H.R. 1127 includes veterinary medicine in its definition of "medical." The EPC, however, clearly treats animal and human medical processes alike.

203. *Id.* § V, ¶¶ 3.1, 3.2, 3.3.

204. *Id.* § V, ¶ 3.5.

weight was not an "industrial application" but "merely a consequence of the therapeutic treatment."²⁰⁵ Clearly, in this and a number of other situations,²⁰⁶ the distinctions between industrial and medical (that is, between advances which require the incentive of patent protection and those that do not) may be difficult to justify or even explain.

The logical question, then, is by what other criteria may the patents that raise ethical objections be distinguished from the patents that do not? Or, more appropriately phrased: What else about medical process claims makes them the target of the medical community and the proposed legislation? The arguments that product and "new use" inventions are often more costly to develop or are more "tangible" in a way that merits protection²⁰⁷ are often inaccurate and hence, as *In re Bayer AG* demonstrates, difficult to rationalize.

Perhaps the distinction lies not so much in the claimed subject matter, but in the professional role of the inventor. Physicians, logically enough, are most often the inventors of medical processes and "new uses," but rarely develop new pharmaceuticals or devices.²⁰⁸ Thus, even though they are rarely expert synthetic chemists or mechanics, physicians are in a unique position to "experiment" with novel uses for known technologies and explore new surgical and therapeutic processes. In this regard, it is interesting to note that before what may be termed the "compartmentalization" of medicine (with synthetic chemists or mechanics working alone on their inventions, far from the hospital), physician-inventors were more closely involved in the development of all medical technologies.²⁰⁹ Perhaps, then, it is not mere coincidence that the AMA's long-forgotten prohibitions against the patenting of any medical innovation were in force during the time when physicians typically invented all types of medical patents. I suggest that as the role of physician-inventors in developing medical products disappeared, the

205. *Id.* § V, ¶ 7.

206. See *Hearings, supra* note 31 (testimony of Dr. William D. Noonan). Dr. Noonan testified that "European patent practice allows a new use of a known drug to be patented as a 'composition for use in the treatment' of a pathological condition" in spite of the ban against patents protecting methods of treating the human or animal body.

207. In fact, proponents of the House bill have made this argument. *Hearings, supra* note 31 (testimony of Dr. H. Dunbar Hoskins, Jr. and Dr. Jack A. Singer).

208. *Hearings, supra* note 31 (testimony of Dr. Charles D. Kelman). Dr. Kelman testified that "the advancements [in medical procedures] occur through gradual, on-the-job improvements and refinements of known methods in operating rooms and physicians' offices."

209. See PALMER, *supra* note 27 (providing a thorough analysis of medical patent policies for the first three decades of the twentieth century).

prohibitions against such patents became far less severe. Now that practicing physicians rarely develop medical products on their own, objections to the patenting of medical products are rarely voiced.²¹⁰

This modern reality coupled with the lack of important differences between "objectionable" and "non-objectionable" medical patents leads to the conclusion that the only relevant distinction, with respect to ethical or conflict-of-interest concerns, lies in who owns (and is therefore empowered to enforce) the patent rights. The most serious ethical objections are raised only where physician-inventors own, license and attempt to enforce their own medical patents, or where physicians have interdependent relationships with other medical patent owners.

Very often, however, physician-inventors must assign all of their patent rights to the institutions for which they work and do not play an active role in the licensing or enforcement of the patent. At university medical centers this was an accepted, if rare, practice until passage of the Bayh-Dole Act in 1980.²¹¹ After that legislation allowed patents to issue for the inventions developed with the aid of federal grants, nearly all major university medical centers created technology transfer administrations.²¹² These administrations have served a valuable role by creating incentives to pursue both basic and applied research, reducing the costs of individual licensing transactions, and fostering cooperation between academia and industry.²¹³ Unlike individual inventors, technology transfer administrations have strong incentives, both internal and external, to share medical technology. Because relatively large organizations

210. See *supra* part V.A.

211. Pub. L. No. 96-517, 94 Stat. 3019 (1980) (codified as 35 U.S.C. §§ 200-212 (1988)) ("Chapter 18. Patent Rights in the Inventions Made with Federal Assistance").

212. GARY W. MATKIN, AMERICAN COUNCIL ON EDUCATION, TECHNOLOGY TRANSFER AND THE UNIVERSITY (1990) (citing Gary W. Matkin, *Technology Transfer and the American Research University* (1989) (unpublished Ph.D. dissertation, University of California (Berkeley))). See generally Reid G. Adler, *Technology Transfer, Government Research, and the Frontiers of Science: Intellectual Property Protection in the Biotechnology Industry*, 39 FED. BAR NEWS & J. 270 (1992); Brian J. Reichel, *Regulating Conflicts of Interest in the Technology Transfer Age: Promoting Public Trust Or Defeating Public Interest?*, 40 DRAKE L. REV. 385, 398-402 (1991) (summarizing the history of private, public and federal technology transfer administrations).

213. See 60 Fed. Reg. 12,771 (1995) (National Institutes of Health's (NIH) Uniform Biological Materials Agreement (UBMTA)). See also Richard Stone, . . . *While NIH Unveils a Tech Transfer Treaty*, 268 SCIENCE 19 (1995) (discussing the NIH-UBMTA and claiming it will speed the transfer of proprietary materials); Arthur George et al., *The Commercial Campus*, THE RECORDER (SAN FRANCISCO, CA), INTELLECTUAL PROPERTY SUPPLEMENT, Mar. 6, 1995, at 38 (discussing evolving role of university technology transfer administrations) (on file with author).

must constantly license "in" a variety of patented technologies for their own members to use, they are far less likely to refuse to license "out" any single patented technology than an independent physician-inventor with a narrow specialty would be.²¹⁴ Also, institutional technology transfer administrators are subject to the scrutiny of academic researchers, who may value and enforce the "sharing norm."²¹⁵ For these reasons, and because institutional technology transfer may be a more efficient means of recovering the costs of research and development than independent inventors licensing their own patent rights, nearly all major research centers now have some form of technology transfer administration.²¹⁶

VI. A PROPOSAL: MANDATORY ASSIGNMENT OF PHYSICIANS' PATENT RIGHTS

The central dilemmas facing independent physician-inventors, then, are that the patent system provides incentives for them to disregard the "sharing norm" of medical science and to overlook their ethical and fiduciary duties to patients. The "sharing norm" and the concerns raised by breaches of a fiduciary duty do not confront the inventors of most medical products because "sharing" is no longer a strong ethical norm in the industries most often involved with the development of pharmaceuticals or medical devices. Likewise, these inventors owe no meaningful fiduciary duty to individual patients. The enforcement of patent rights may also lead physicians to disregard their ethical obligations to preserve patients' privacy and autonomy.

The pending legislation and the current AMA Principles of Medical Ethics tacitly recognize that only non-physicians are responsible for the development of medical products, by admitting that patenting such inventions is ethical and in fact should be encouraged. In seeking to impose a "sharing norm" on *only* physician-inventors, the medical community has overreacted, attempting either to outlaw all the patents physician-inventors would typically own or to prevent the enforcement of their patent rights. In so doing, the medical community has overlooked a far less drastic alternative: entrusting the enforcement of the "sharing norm" and the associated ethical and fiduciary duties to organizations subject to the oversight of the medical community.

214. I am not aware of any empirical evidence that supports this assertion, but I suggest the underlying logic is compelling.

215. See *supra* part II.A.

216. MATKIN, *supra* note 212. See also Adler, *supra* note 212, at 270.

In June of 1914, the House of Delegates of the AMA gave permission to the association's Board of Trustees "to accept, at their discretion, patents for medical and surgical instruments and appliances and to keep these patents as trustees for the benefit of the profession and the public; provided neither the [AMA] nor the patentee shall receive remuneration from these patents."²¹⁷ At that time few (or no) medical process patents were issued by the PTO, and the AMA strongly disapproved physician-owned patents of any kind. Nevertheless, the AMA could have held itself out as a repository for medical patents developed by concerned non-members. It appears that too few of these generous inventors stepped forward and that even fewer physicians were willing to offer evidence that they had violated the AMA's ethical code. Thus, the AMA never became the national medical patent clearinghouse the House of Delegates may have envisioned.

A. Patent Clearinghouses for Physician-Invented Patents

I have argued that the current debate over the patentability of medical processes and the ethical and conflict-of-interest objections raised by these patents are, by and large, merely objections to the ownership and enforcement of patents by practicing physicians.²¹⁸ A mandatory assignment system limited to physician-inventors, therefore, could resolve much of the current debate. Such a mandatory assignment system, in which incentives to invent coexisted with safeguards against the violation of ethical norms, can be easily envisioned.

Organizations subject to the governance of a significant portion of the medical community (much like the AMA) could manage patent clearinghouses for the rights of otherwise independent physician-inventors. To ensure that all physicians participated in a clearinghouse, each organization would have to be approved by various state medical licensing boards. Furthermore, as a requirement to licensure, every physician would be required to assign any patent rights to one of the several state-approved clearinghouses. A university-affiliated physician would have the option of assigning her patent rights to the university, if it had been approved by the state.

Certain uniform rules would apply to all of the clearinghouses. Each would be required to offer all of its rights as a package to

217. Fishbein, *supra* note 6, at 1317 (discussing proposal of 1914). Also described in Sperry, *supra* note 27, at 372 and in PALMER, *supra* note 27.

218. See *supra* part V.D.

medical centers throughout the country. While each could employ different formulas to determine licensing rates, those rates would reflect only the size, location, or specialty of a potential licensee medical center, *not* the number of times a specific invention has been used by that hospital in the past. Meanwhile, member physician-inventors would be reimbursed on a per-use basis, and only medical records containing no identifiable information about individual patients (e.g., physicians' medical malpractice insurance records or hospitals' operating room logs) would be used to confirm the number of times a specific product or process was used. In this way, the invasions of patients' rights to privacy that most often result from enforcement of a patent could be avoided.²¹⁹

However, the details of each clearinghouse's licensing and enforcement scheme could be left to the individual organizations. For example, universities likely would simply retain their present technology transfer offices, but other organizations could look to their membership to strike an appropriate balance between profits and generosity. This variety would allow each physician to select an appropriate clearinghouse for his particular needs and desires. For example, if a physician wishes to license any future invention freely, he would select an appropriate clearinghouse. If, however, he wishes to recover research costs through patent rights, he could choose a clearinghouse with an appropriate licensing structure. Thus, by modeling their activities on existing technology transfer administrations, the proposed patent clearinghouses could become players in a dynamic market.

This proposal finds support in the basic fact that the PTO, when judging the patentability of an invention, is no longer inclined or empowered to enforce society's (much less a given profession's) ethical norms.²²⁰ At the administrative level, such determinations are now

219. Comment, *Medical Process Patents and Patient Privacy Rights*, 14 J. COMPUTER. & INFO. L. 131, 147 (1995) (noting that Montana and Washington have recently enacted modified versions of the 1985 Uniform Health-Care Information Act to protect the confidentiality of medical records). See also MONT. CODE ANN. §§ 50-16-501 to 553 (1987) (Uniform Health Care Information); WASH. REV. CODE ANN. §§ 70.02.005-904 (West 1991) (Medical Records-Health Care Information Access and Disclosure).

220. Merges, *Controversial Technologies*, *supra* note 90, at 1062-68 (concluding that patent protection for a new technology "normally should not be denied on the basis of speculation about potential negative consequences" and that other agencies such as the FDA are better suited to evaluate the potential deleterious effects of new medical technologies). For a more current analysis of the appropriate roles of the PTO and FDA, see *In re Brana*, 51 F.3d 1560, 1564 (Fed. Cir. 1995) (citing the PTO's "Guidelines for Examination of Applications for Compliance with the Utility Requirement," 60 Fed. Reg. 97 (1995)).

often left to the FDA,²²¹ an agency not answerable to the medical community. The direct control exercised by the medical community over the patent clearinghouses, however, should make the proposed system far more attractive to physicians than either the present system or the proposed legislation's inelegant barriers to the patenting of "pure" medical processes. Additionally, under the proposed system the AMA would play an active role in promoting and assessing new medical technologies. Under both the present system and that of H.R. 1127, the AMA plays no such role.

At yet another level, the proposal creates an enforcement mechanism for the medical community's ethical stance on medical patents. Because boards composed of members of both the medical and research communities could determine rates of compensation for physician-inventors, a physician-inventor's licensing profits need never be so great as to "retard or inhibit research or restrict [social] benefits."²²² The rates at each clearinghouse could be set to strike an appropriate balance among three competing parameters: (1) physician-inventors' desire to recover costs of research and development, (2) physician-inventors' desire to profit from their inventions by extracting a portion of the savings their inventions have afforded society, and (3) the "local" community's desire to provide medical services at the lowest possible cost while still spurring inventions that lead to greater cost savings. The third factor may be seen as a means by which the patent clearinghouse could promote the development of technologies needed to serve society's most basic medical needs by encouraging the development of cost-saving technologies while discouraging the development of certain cost-intensive technologies.

Applying this three-factor rate-setting analysis to the controversial case of Dr. Samuel Pallin,²²³ his clearinghouse might have considered: (1) that Pallin expended virtually no resources in developing his patented incision; (2) that Pallin justifiably desires to extract some of the \$17 his procedure saves each patient; and (3) that there are societal and economic values in reducing the cost of cataract surgery. Balancing these interests in a meaningful way, the clearinghouse could arrive at a reasonable fee at which to reimburse Pallin each time his operation is performed. Such a fee (set, for example, at \$1) would be multiplied by the number of times Pallin's incision is performed over the course of a year (100,000), netting Dr.

221. See *supra* part IV.

222. AMA PRINCIPLES OF MEDICAL ETHICS, 11-12, § 7 (1955) ("Patents and Copyrights").

223. See *supra* part II.

Pallin a handsome reward (nearly \$2 million) during the term of his patent.

Of course, the proposed collection of patent clearinghouses would not resolve all of the ethical and conflict-of-interest concerns raised by medical patents. Pharmaceutical and medical device manufacturers, with justifiable interests in recovering large investments, are often forced to price the latest innovations beyond the financial reach of many patients. Likewise, physicians' conflicts of interest are only partially allayed by the proposed system. While many perverse incentives created by physician-owned patents are eliminated under the proposed system, ties between physician and other holders of medical patents will still raise considerable concerns. The proposal, nonetheless, accomplishes its goal. It reconciles the medical community's need to enforce ethical and professional norms on its members while preserving many incentives to invent and disclose new and more effective medical technologies.

B. ASCAP as a Model for the Patent Clearinghouses

The reader may have already observed that the proposed medical patent clearinghouses closely resemble current copyright clearinghouses, such as the American Society of Composers, Authors, and Publishers (ASCAP) and Broadcast Music, Inc. (BMI). The ASCAP model,²²⁴ a more appropriate model for the proposed patent clearinghouse system, offers four distinct benefits aside from allowing the medical community to enforce its own ethical and professional norms. The proposed system, if closely modeled on ASCAP, will provide for the selling of "blanket" licenses (so called because a single license covers an entire portfolio of rights) to physicians and medical centers. The cost of these licenses would be based only on a medical center's size, specialty, or location. Such a pricing structure would better protect the privacy of patients, for there would be no need to inspect licensee operating rooms for potential infringements. Just as ASCAP uses radio station play lists to calculate only correct disbursements to its members, the medical patent clearinghouses would collect anonymous operating room or laboratory reports to

224. ASCAP represents more than 40,000 members and controls a repertoire of approximately 3 million compositions. Composers, authors and publishers who are members of ASCAP assign their copyrights to the organization in exchange for perpetual royalties, ASCAP's licensing and enforcement services, and representation in ASCAP's governance. For a brief description of ASCAP, its competitor BMI, and their respective methods of operation, see Janet L. Avery, *The Struggle Over Performing Rights To Music: BMI and ASCAP vs. Cable Television*, 14 HASTINGS COMM. & ENT. L.J. 47, 51-53 (1991).

calculate disbursements to physician-inventors. This efficient means of calculating royalties and enforcing patients' privacy rights could compensate inventors such as Dr. Pallin for the correct number of times his procedure was used, while not requiring that hospitals be secretly monitored.²²⁵

A secondary, but compelling, benefit lies in the patent clearinghouse's ability to reduce transactional costs and, in so doing, potentially reduce the cost of medical care in general. All of the individualized licensing, disbursement and enforcement costs that would discourage an otherwise capable physician-inventor from pursuing a new technology would virtually disappear under the proposed system. This physician-inventor, no longer concerned by the costs or stigma of enforcement and assured an equitable return for successful innovative efforts, could focus on developing new, less-costly medical procedures. Additionally, the removal of independent patent holders from licensing negotiations would reduce the number of "hold-outs" who refuse to license technology for a reasonable fee, while eliminating many of the costs of repetitive negotiations.

These latter two additional benefits of the ASCAP model, though more subtle, are no less important. At least part of ASCAP's appeal to its members lies in the organization's willingness to take care of the more "distasteful" business aspects of artists' lives. As far as many members are concerned, if ASCAP affords them suitable royalties while also negotiating licenses, monitoring users, and policing their rights, that is all the better. Similarly, physician-inventors, freed of the more mundane concerns of managing their patent rights, could concentrate more fully on their craft: healing the sick.

A fourth benefit of the ASCAP model is inextricably tied to the other three. One of ASCAP's principal attractions to its members is its representative form of governance. The presence of a representative board of directors, to set both fees and policy, helps guarantee equitable distribution of the proceeds of the licensing agreements while reassuring all members that they have a voice in the organization. Physician-members of the central patent clearinghouse would also benefit from such a system of governance.

225. Of course, "spot checks" limited to verifying operating room logs might be required in exceptional circumstances. Nevertheless, an individual hospital would have no incentive to falsify its logs because the blanket licensing fee would be set independently of uses; it would be based only on the size, location, or specialty of the hospital.

VII. CONCLUSION

The current debate over the propriety of allowing medical process patents, which has worked its way into the U.S. Congress, has provided both the medical and patent law communities an opportunity to examine their current policies. While both communities' policies may be directed toward the same goal, that of providing patients the best and most advanced care at the lowest possible cost, each community pursues distinct, often conflicting, means to that end. The patent system presents powerful incentives to invent and disclose new and useful medical technologies, but it fails to adequately address concerns regarding physicians' adherence to their own code of ethics and their respect for the fiduciary duties owed their patients. This failure indicates that a complete "sacrifice" of medical technologies to the principles underlying the patent law would be unwise.²²⁶ Just as the enforcement of injunctions to enforce patent-holders' rights is always subject to the dictates of public policy,²²⁷ the degree to which patent rights are vested in physician-inventors should be monitored with an eye on the concerns of medical ethics and on the avoidance of conflicts of interest. To the extent that the present patent system provides incentives for physicians to disregard their own professional code of ethics and to breach the fiduciary duties owed their patients, that system should be modified.

At the same time, the medical community values its own ethical and professional standards but disregards the long-term benefits of the patent system. By undervaluing the incentives created by medical process patents, the AMA does a disservice to physician-inventors and to society in general. By completely eliminating medical process patents, the proposed legislation would create perverse incentives for physicians to conceal their discoveries and to abandon promising, though unconventional, new treatments. The proposed legislation would introduce these harms but would address only a few of the ethical and conflict-of-interest concerns raised by medical patents.

The proposal I advance is not entirely novel,²²⁸ but it does provide a viable solution to the impasse between current views in the medical community and the justifications of the patent system. It

226. For a related analysis, suggesting that patent policy should be adapted to the special concerns raised by medical innovation, see Evan Ackiron, Note, *Patents for Critical Pharmaceuticals: The AZT Case*, 17 AM. J.L. & MED. 145 (1991).

227. *Roche Prods. v. Bolar Pharmaceutical Co.*, 733 F.2d 858 (Fed. Cir.), cert. denied, 469 U.S. 856 (1984).

228. Fishbein, *supra* note 6, at 1317. Also described in Sperry, *supra* note 27, at 372 and in PALMER, *supra* note 27.

modifies the present patent system by shifting the burden of distributing and enforcing physician-invented technologies from independent physicians to institutions better suited to that task. It also vests the power to enforce norms of medical ethics and professionalism in organizations answerable to their members, the medical community. Moreover, the proposal represents a meaningful compromise between the positions of the medical community and the strongest proponents of the patent system by placing an efficient enforcement mechanism at the disposal of the medical community. This modified enforcement structure would also safeguard the privacy concerns of patients. Thus, while the proposal does preserve many of the patent system's desirable incentives to invent, it also recognizes the role the medical community must play in enforcing the ethical norms of the profession.

COMMENT

A BEHAVIOR-BASED MODEL FOR DETERMINING SOFTWARE COPYRIGHT INFRINGEMENT

DENNIS M. CARLETON †

TABLE OF CONTENTS

I.	INTRODUCTION	405
II.	DEFINING COMPUTER PROGRAM BEHAVIOR	408
III.	FITTING COMPUTER PROGRAMS WITHIN TRADITIONAL COPYRIGHT LAW	409
	A. Behavior Is Expression	409
	B. Why Behavior Is Protectable	411
	C. Limitations On Protection Of Behavior	416
	D. Computer Programs As Useful Articles	418
IV.	RELEVANT CASE LAW	420
V.	THE PROPOSED BEHAVIOR-BASED TEST	425
VI.	AN APPLICATION OF THE PROPOSED BEHAVIOR-BASED TEST	430
VII.	CONCLUSION	432

I. INTRODUCTION

In 1980, Congress amended the Copyright Act to explicitly recognize copyright protection for computer programs.¹ However, Congress left the task of determining the proper scope of such protection

© Dennis M. Carleton.

† J.D. Candidate, 1996, University of Pittsburgh School of Law; 1983, Master of Software Engineering, Carnegie-Mellon University; 1990, BSEE, Carnegie-Mellon University. The author has ten years of professional software engineering experience. Special thanks to Professor Pamela Samuelson of the University of Pittsburgh School of Law for her comments and help.

1. Pub. L. No. 96-517 § 10(a) (1980) U.S.C.A.A.N. 94 Stat. 3028. The 1980 amendments changed the Copyright Act by adding a definition of "computer program" to section 101, and by adding section 117, which grants certain rights to users of computer programs.

to the courts, providing only that the courts maintain the traditional distinction between idea and expression.²

Since then, courts have grappled with copyright protection for computer programs with mixed results.³ The primary struggle surrounds the extent of copyright protection for "non-literal" aspects of computer programs.⁴ This article suggests that program behavior⁵ must be protected as a non-literal aspect of the program. Furthermore, any test for copyright infringement, absent readily provable literal copying of the programmer's source code, should look solely to the behavioral aspects of the program to determine whether infringement has occurred, eschewing any analysis that dissects a program's structure, organization and other elements related to the programming code.

There are several reasons for advocating this "black box"⁶ type of analysis. First, computer programs are included under the Copyright Act as literary works. As such, they should receive the same level of protection that is extended to other literary works. Thus, the traditional copyright principles and doctrines which protect the non-literal aspects of other literary works should also protect the non-literal aspects of the programmer's expression. Second, the underlying purpose of the Copyright Act supports the protection of program behavior. The behavior of a program is the only aspect of the programmer's expression that is perceived and valued by users. Unless the programmer receives protection from copying of program behavior, the programmer's incentive for producing creative works will be diminished. Finally, there are many ways to write and structure a program so that it will behave in a particular way. As a result, any test for non-literal infringement limited to dissecting the programming code, organization and structure will fail

2. *Id.* The 1980 amendments to the Copyright Act adopted almost verbatim the recommendations of the NATIONAL COMMISSION OF NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT (1979) [hereinafter CONTU REPORT]. The report called for the courts to determine the protectible elements of software. CONTU REPORT, 18.

3. See Irwin R. Gross, *A New Framework For Software Protection: Distinguishing Between Interactive And Non-Interactive Aspects Of Computer Programs*, 20 RUTGERS COMPUTER & TECH. L. J. 107, 132 n.113 (1994).

4. Non-literal aspects of computer programs are "those aspects that are not reduced to written code." *Computer Assoc. v. Altai Inc.*, 982 F.2d 693, 696 (2d Cir. 1992).

5. For a discussion of the definition of the behavior of a computer program, see *infra* part II.

6. The term "black box," as used in computer science, describes the method of software testing whereby the functional interface of the software is tested without knowledge of or regard for the internal implementation of the functions of the program. Compare ROGER S. PRESSMAN, *SOFTWARE ENGINEERING: A PRACTITIONER'S APPROACH* 470, 484 (2nd ed. 1987) and RICHARD E. FAIRLEY, *SOFTWARE ENGINEERING CONCEPTS* 284 (1985) with Duncan M. Davidson, *Common Law, Uncommon Software*, 47 U. PITT. L. REV. 1037, 1080 (1986) (using the term "black box" in a slightly different context to support the notion that external attributes of a program "should be considered completely reverse engineerable").

to detect copying of the original work, thus undermining the protection offered by copyright.

To date, the courts have been uneven in their treatment of copyright protection for program behavior. In many cases, courts have extended copyright protection to behavioral elements of computer programs, accepting the notion that computer programs ought to receive the same degree of protection from non-literal copying as provided to other literary works.⁷ Other courts, however, have held that program behavior ought to be excluded from the inquiry into non-literal infringement, and have limited their analyses to the non-literal elements of the source code.⁸

The first part of this article develops the reasons for advocating a behavior-based test for determining software copyright infringement, starting with an analysis of the problem in light of traditional copyright doctrine, the Copyright Act of 1976 and congressional intent. Next, the article analyzes how the courts have struggled with the concept of non-literal infringement of computer programs. Most courts appear to be moving toward the Abstraction-Filtration-Comparison (AFC) test which was formulated by the Second Circuit in *Computer Associates International v. Altai*.⁹ While most courts agree on the test, they disagree over its proper application. This article suggests a behavior-based test which modifies the Abstraction-Filtration-Comparison test. The test proposed by this article would eliminate the "abstraction" step of the AFC test, which involves separating the levels of abstraction within the program's code, organization and structure. Instead, the behavior-based test would replace the abstraction step with an "identification" step, which dissects

7. See, e.g., *Whelan Assoc. Inc. v. Jaslow Dental Lab.*, 797 F.2d 1222 (3d Cir. 1986), *cert. denied*, 479 U.S. 1031 (1987) (holding non-literal aspects of program copyrightable); *Broderbund Software v. Unison World, Inc.*, 648 F. Supp. 1127 (N.D. Cal. 1986) (holding sequence of screens, computer screen displays protectable); *Manufacturers Technologies v. Cams, Inc.*, 706 F. Supp. 984, 993 (D. Conn. 1989) (concluding that program's copyright protected the literal and non-literal elements of the program's screen displays, user interface and structure to the extent that each contains copyrightable subject matter); *CMAX/Cleveland v. UCR*, 804 F. Supp. 337 (M.D. Ga. 1992) (holding screen displays and reports were protectable expression); *Apple Computer v. Microsoft Corp.*, 35 F.3d 1435 (9th Cir. 1994) (holding "look and feel" of user interface not protectable expression apart from individual elements of interface); *Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568 (S.D. Fla. 1994) (extending protection to text of commands and the way the program looked, sounded, and interacted with the user); *Autoskill, Inc. v. Nat'l Educ. Support Sys.*, 994 F.2d 1476 (10th Cir. 1993), *cert. denied*, 114 S.Ct. 307 (1994) (finding infringement in reading testing program where infringer had merely changed the names and sequences of the tests and made minor format changes); *Napoli v. Sears, Roebuck and Co.*, 874 F. Supp. 206 (N.D. Ill. 1995) (holding that copyright extends to computer screen displays).

8. See, e.g., *Brown Bag Software v. Symantec*, 960 F.2d 1465 (9th Cir.), *cert. denied*, 113 S. Ct. 198 (1992); *Gates Rubber Co. v. Bando Chemical Indus.*, 9 F.3d 823 (10th Cir. 1993); *Lotus Dev. v. Borland Int'l*, 49 F.3d 807 (1st Cir. 1995), *cert. granted*, 116 S.Ct. 39 (1995).

9. 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part, remanded*, 982 F.2d 693 (2d Cir. 1992).

and identifies the elements of the program's behavior. The behavior-based test would eliminate much of the confusion and difficulty involved with applying the AFC test. Finally, the article applies the proposed test to the facts in *Lotus Development Corp. v. Borland International* to illustrate its advantages. Developing a workable test for non-literal infringement of computer software has become especially relevant in light of the Supreme Court's recent grant of certiorari in the *Lotus* case.¹⁰

II. DEFINING COMPUTER PROGRAM BEHAVIOR

Before beginning any discussion of a test for copyright infringement based on the behavior of computer programs, it will first be necessary to define "program behavior." For purposes of this article, a program's behavior consists of the appearance of the user interface, the way in which the user interacts with the program, the manner in which information is input to and output from the program, and the ensemble of functions provided by the program. In short, it is everything that happens once the program is executed on the target system.

The behavior of a program may be quantified in terms of discrete elements. These elements include the discrete functions performed by the program, specific features of the program's user interface, or particular program responses to a user's actions. A program's behavior can thus be summarized as the set containing all the discrete behavioral elements. Some simple examples of discrete behavioral elements include the manner in which the program responds to specific inputs, such as the invocation of a command by a user, or a signal from the printer indicating that it has run out of paper. A program's response may be expressed as a change in the appearance of the screen, the posting of error messages, or the emission of a beep or other audible signal. Behavior also includes a program's expression in the absence of any input, such as a screen saver program which posts a fluctuating pattern on the computer's screen when the user does nothing. Many programs have very limited or almost no interaction with users, yet still exhibit behavior. An example of this would be a program that controls traffic lights.

10. 116 S.Ct. 39 (1995).

III. FITTING COMPUTER PROGRAMS WITHIN TRADITIONAL COPYRIGHT LAW

A. Behavior Is Expression

In order to be copyrightable, the subject matter must be an "original work of authorship fixed in any tangible medium of expression."¹¹ Copyright law protects an author's expression, rather than merely the idea being expressed. The expression of an idea takes on both substance and form. The substance of the expression lies in the distinction between the author's expression and the ideas which are being expressed. This is the essence of the traditional idea/expression dichotomy of copyright law.¹²

In most cases, the form of the author's expression is readily apparent. For example, the expression of the author of a novel is manifested in the form of printed words on the page. The form of the author's expression, however, can have multiple manifestations, raising the question as to the extent of copyright protection for each distinct manifestation.

The form of the computer programmer's expression can be divided into two distinct manifestations: the literal and the behavioral.¹³ The literal manifestation consists of the text of the human-readable program as written by the programmer (i.e., the source code).¹⁴ The behavioral manifestation consists of the dynamic form of the program as it is being operated on a computer.¹⁵ This bifurcation of expression is neither a new concept nor one unique to computer programs.¹⁶ Consider the various forms of expression of a musical work. The sheet music embodies the literal manifestation of the composer's expression, while the performance of the musical piece makes up the "behavioral" manifestation of that

11. 17 U.S.C. § 102(a) (1988).

12. See *Baker v. Selden*, 101 U.S. 99 (1880); 17 U.S.C. § 102(b) (1988) (codifying the holding of *Baker*, and the idea/expression dichotomy).

13. At least one commentator has expressed the difference as that between interactive and non-interactive elements of the program, defining interactive elements as those which are "directly perceived by humans in the course of using the program." Gross, *supra* note 3, at 112-15.

14. Source code is defined as symbolic coding in its original form before being processed by a computer. The computer automatically translates source code into a code it can understand by a process called "compiling." DONALD SPENCER, WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 539 (5th ed. 1994) [hereinafter WEBSTER'S DICTIONARY OF COMPUTER TERMS].

15. See *supra* part II for a definition of behavior of a computer program.

16. See Pamela Samuelson, *CONTU Revisited: The Case Against Copyright Protection for Computer Programs in Machine-Readable Form*, 1984 DUKE L. J. 663 n.320-22 and accompanying text.

same musical work. Both manifestations are merely alternative forms of the same expression. Thus, each manifestation of the expression should be protected by copyright, because both are a part of the same "original work of authorship." In the case of the musical composition, no one doubts the conclusion that both forms of expression are protected by copyright. The unauthorized public performance of a musical composition infringes the composer's copyright, as does the copying of the sheet music.¹⁷ By analogy, the same reasoning should hold true for computer programs—copying of program behavior infringes the programmer's copyright, as does the copying of the source code.

Computer programs, however, differ from most other literary works in that they derive most of their value from the behavioral form and not from the specific manner in which the programmer implemented the behavior.¹⁸ The behavior of a program may provide a solution to a problem, offer entertainment, or serve as a tool which the user can employ to do valuable work. Consumers would not want to buy a program that does not "behave, i.e., that [does] nothing."¹⁹ Consumers care only about the benefit derived from how the program behaves; the literal manner in which the programmer has implemented the behavior is of little consequence to the consumer.

The literal manifestation of the programmer's expression, on the other hand, only has value to the programmer, who can modify it to maintain and enhance the behavior in subsequent versions of the program.²⁰ Consumers value a program "not because they have any intrinsic interest in what its text says, but because they value what it does and how well it does it."²¹ When a consumer buys a program, he buys only the program's behavior, not the text of the program's source code.²² The consumer cannot directly perceive the programmer's expression from the literal text of the program, because it is invisible to him. Thus, the program behavior represents to the consumer the totality of the programmer's expression.

Given that programs derive so much of their value from their behavioral manifestation, and given that consumers do not perceive the

17. 17 U.S.C. § 106(1) (1988) (providing the author the exclusive right "to reproduce the copyrighted work in copies or phonorecords") and 17 U.S.C. § 106(4) (1988) (providing the author the exclusive right "to perform the copyrighted work publicly").

18. See Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2317 (1994) [hereinafter *Manifesto*].

19. *Id.* at 2315.

20. See Gross, *supra* note 3, at 114-15 ("[T]ypical computer users care very little about a program's non-interactive elements so long as they function properly.").

21. *Manifesto*, *supra* note 18, at 2318.

22. *Id.*

literal manifestation of the program, the emphasis of copyright protection should be aimed at program behavior rather than the written source code.

B. Why Behavior Is Protectable

1. THE 1980 CHANGES TO THE COPYRIGHT STATUTE

When computer programs were explicitly added to the copyright statute in 1980, Congress expressed its intent that such works should be treated as literary works.²³ Though the Copyright Act's definition of a literary works does not expressly list computer programs, the definition clearly encompasses a typical computer program.²⁴ The definition of literary works includes "works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied."²⁵ In addition, a 1976 congressional report explicitly discussed treating computer programs as literary works "to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves."²⁶

Some confusion over the protectability of program behavior may stem from section 101 of the Copyright Act, which defines a computer program as "a set of statements or instructions used directly or indirectly in a computer to bring about a certain result."²⁷ A strict reading of section 101 might suggest that a computer program for copyright purposes is limited to the written source code because the definition under the Act does not expressly refer to a program's behavior or dynamic structure. Yet, the absence of a direct reference to program behavior under section 101 should not be determinative. The language of section 101 can be

23. See CONTU REPORT, *supra* note 2, 18-23. The Congressional Commission on New Technological Uses of Copyrighted Works recommended that the copyright statute be amended to provide protection for computer programs as both literary and audiovisual works. Congress adopted CONTU's recommendations essentially verbatim.

24. A computer program is defined as a formal expression of the sequence of actions required for a data processing task; the programmer's specification of the task(s) to the computer in a formal notation that can be processed by the computer. It consists of a series of statements and instructions that cause a computer to do a specific job. WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 117.

25. 35 U.S.C. § 101 (1988) (definition of "[l]iterary work").

26. H.R. REP. NO. 1476, 94th Cong., 2d Sess. 54 (1976), *reprinted in* 1976 U.S.C.A.N. 5659, 5667 (protecting computer programs as literary works to the extent they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves).

27. 17 U.S.C. § 101 (1988).

interpreted as referring to program behavior indirectly through the phrase "to bring about a certain result."

Furthermore, the use of the defined term "computer program" is conspicuously absent in the section of the Copyright Act defining protectable subject matter, implying that Congress did not intend for computer programs to be treated any differently than other types of literary works. Had Congress intended to limit copyright protection for computer programs as compared to other copyrightable works, it could easily have done so by creating a separate category for computer programs under section 102.²⁸ However, no such attempt was made. The term "computer program" is in fact only used in the copyright statute in section 117,²⁹ which exempts RAM copies created in the owner's operation of a program and copies made for backup purposes from being deemed infringing of the programmer's copyright.³⁰

2. QUASI-LEGISLATIVE HISTORY

Many commentators consider the National Commission of New Technological Uses of Copyrighted Works, Final Report,³¹ (the CONTU Report) to be the quasi-legislative history of the 1980 amendments to the Copyright Act.³² Although not binding, many courts have accepted the report as evidence of congressional intent because the recommendations contained in the CONTU Report were adopted by Congress without alteration.³³ At the time that CONTU prepared its report, "it had been well-established for decades that copyright protection (for literary works)

28. 17 U.S.C. § 102 (1988).

29. 17 U.S.C. § 117 (1988).

30. The statute provides:

Notwithstanding the provisions of § 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:

(1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or

(2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

Id.

31. See CONTU REPORT, *supra* note 2, 18-23.

32. See Arthur J. Levine, *Comment on Bonito Boats Follow-Up: The Likely Rejection of Nonliteral Software Copyright Protection*, 6 COMPUTER L. 29, 31 (1989); *Micro-Sparc, Inc. v. Amtype Corp.*, 592 F. Supp. 33, 35 n.7 (D. Mass. 1984) ("The CONTU Report . . . comprises the entire Legislative history of § 117.").

33. *Whelan Assoc. Inc. v. Jaslow Dental Lab*, 797 F.2d 1222, 1241 (3d Cir. 1986).

extends to non-literal copying as well as to literal copying.³⁴ Thus, had CONTU intended to apply a different standard for determining non-literal infringement for computer programs than for other forms of literary works, the commission could have recommended this in its report. Yet, the CONTU Report recommended that programs be protected as literary works, without any qualification.³⁵ The report expressed the belief that existing copyright principles were adequate for the task of protecting computer programs, suggesting that courts were better equipped than Congress to develop the law through case-by-case decisions, rather than by shortsighted legislative fiat.³⁶

The CONTU commissioners recognized the problem of distinguishing between idea and expression when dealing with a computer program:

Drawing the line between the copyrightable form of a program and the uncopyrightable process which it implements is simple [for pure literal copying]. But the many ways in which programs are . . . used . . . and the new applications which advancing technology will supply may make drawing the line of demarcation more and more difficult. To attempt to establish such a line in this report written in 1978 would be futile. Most infringements, at least in the near future, are likely to involve simply copying . . . Should a line need to be drawn to exclude certain manifestations of programs from copyright, that line should be drawn on a case-by-case basis by the institution designed to make fine distinctions—the federal judiciary.³⁷

The commission's refusal to set a standard has given the courts wide latitude for deciding where the line should be drawn. The fact that commissioners recognized the difficulty in drawing such a line suggests their awareness of the distinction between the literal and behavioral manifestations of computer programs. Had the commissioners wished to exclude the behavior of computer programs from the scope of copyright protection, they would have explicitly done so in their report. Their silence on this point implies the intent to include behavioral aspects of computer programs within the scope of copyright protection. Statements by CONTU Vice-Chairman Melville Nimmer suggest that the above

34. Allen R. Grogan, *Bonito Boats and Whelan: A Simple Contrast Between Patent And Copyright Protection*, 6 *COMPUTER L.* 33, 34 (1989); see also *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930) ("It is essential to any protection of literary property . . . that the right cannot be limited literally to the text, else a plagiarist would escape by immaterial variations.").

35. See CONTU REPORT, *supra* note 2, at 11, 18-23.

36. *Id.* at 21.

37. *Id.* at 23.

interpretation of the CONTU Report is correct.³⁸ Nimmer said he understood CONTU as in no way limiting the application of traditional copyright doctrines to computer programs:

CONTU did not recommend, and did not intend, any change in the continuing applicability to programs of general copyright principles—e.g., as to the copyrightability and infringement—in effect following the enactment of the general revision of the Copyright Act of 1976. The general copyright principles applicable to programs have been, and remain, those which are applicable to novels, plays, directories, dictionaries, textbooks, musical works, maps, motion pictures, sound recordings and other categories of works.³⁹

Thus, CONTU apparently intended that computer programs receive the same level of protection from non-literal infringement as other types of literary works.⁴⁰

3. OTHER LITERARY WORKS WITH BIFURCATED EXPRESSION

Most traditional literary works receive protection from non-literal infringement. Take, for example, "architectural plans, choreography, musical scores, musical editions, and stage direction."⁴¹ All of these works possess bifurcated manifestations of the author's expression, and all receive some degree of copyright protection from non-literal infringement.

Many literary works, besides computer programs, serve primarily utilitarian purposes. Such works include "dictionaries, code books, encyclopedias, advertising, and 'how to' instruction manuals, that, like many computer programs, have a primarily utilitarian, rather than aesthetic, entertainment, or educational purpose."⁴² Copyright nevertheless protects both the literal manifestations and the non-literal

38. See Melville Nimmer, *Declaration Regarding the National Commission on New Technological Uses of Copyrighted Works (CONTU) Final Report* (Nov. 15, 1984) reprinted in Anthony L. Clapes et al., *Silicon Epics And Binary Bards: Determining The Proper Scope Of Copyright Protection For Computer Programs*, 34 UCLA L. REV. 1493, app. (1987) [hereinafter *Nimmer Declaration*].

39. *Id.* at ¶12.

40. However, commissioners Miller and Levine disagree with Nimmer on this point. See Steven R. Englund, Note, *Idea, Process, Or Protected Expression?: Determining The Scope Of Copyright Protection Of The Structure Of Computer Programs*, 88 MICH. L. REV. 866, 888-90 (discussion views of commissioners Miller and Levine).

41. Jane C. Ginsburg, Comment, *Four Reasons and a Paradox: The Manifest Superiority of Copyright Over Sui Generis Protection of Computer Software*, 94 COLUM. L. REV. 2559, 2567 (1994).

42. Arthur R. Miller, *Copyright Protection For Computer Programs, Databases, And Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 986 (1993).

aspects of these works.⁴³ Literary works with utilitarian aspects have been "accorded protection since our first Copyright Act in 1790, which embraced maps and charts."⁴⁴ Thus, a computer program, if treated as a literary work as Congress has mandated, should also be accorded protection of its non-literal aspects, the program's behavior, where such aspects represent the programmer's expression.

4. PURPOSE OF COPYRIGHT

Copyright is a tradeoff which grants an author certain exclusive rights to his work in exchange for the disclosure of the work for the public good.⁴⁵ The exclusive rights granted to the author provide the incentive for the author to create. Thus the valuable aspects of the author's work must be protected from copying; otherwise the author's incentive to create will disappear.

A program which behaves in an identical manner or a very similar manner to another program has the potential of becoming a "market substitute"⁴⁶ for the original program. Such programs may potentially degrade the incentive to the programmer because fewer copies of the original program may be sold in favor of substitute programs. Protection of a program's behavior becomes critical because program behavior plays a significant role in marketing a program to potential purchasers.⁴⁷ The user interface of a program, one element of the program's overall behavior, plays a crucial role in helping consumers to "differentiate a program from among similar software applications in a crowded market."⁴⁸ Taking into consideration that the programmer relies on this aspect of expression to distinguish his program from other competing programs, the necessity of protecting the behavioral manifestation of the programmer's expression from copying becomes readily apparent.

43. *Id.* at 986-87.

44. *Id.* at 986. The author also compares computer programs to architectural works and states that the "recently enacted Architectural Works Copyright Protection Act strikingly echoes the present state of computer copyright law." *Id.* at 988 n.45.

45. See 1 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* §§ 3.01-04.

46. *Manifesto*, *supra* note 18, at 2319; see also Gross, *supra* note 3, at 115 n.28 (even programs that are not identical can compete as substitutes).

47. See Bill Curtis, *Engineering Computer "Look and Feel": User Interface Technology and Human Factors Engineering*, 30 *JURI. J.* 51, 53 (1989) (discussing the importance of the use interface in marketing software); see also Garard J. Lewis, Jr., Comment, *Lotus Development Corp. v. Paperback Software International: Broad Copyright Protection For User Interfaces Ignores The Software Industry's Trend Toward Standardization*, 52 *U. PITT. L. REV.* 689, 694-95 n.17 (1991) (citing Curtis).

48. Curtis, *supra* note 47, at 52-54.

Furthermore, limiting copyright protection to program code fails to provide adequate protection for the programmer's creative expression.⁴⁹ Excluding behavior in the determination of non-literal infringement exposes the program's most valuable attributes to copying by any skilled programmer, who could reverse engineer a program by analyzing its behavior and producing an identical or infringing copy without ever viewing the literal source code.⁵⁰ Such reverse engineering often requires only a fraction of the time and labor invested by the programmer of the original work. Ignoring the behavior of a program thus circumvents the very purpose of copyright protection: providing an incentive for the programmer's creative expression for the benefit of the public.

Unlike most other literary works, computer programs are unique in that there is a significant degree of independence between the literal and behavioral manifestations. For most other literary works, the performative manifestation of the work is directly dependent upon the literal manifestation of the work. For example, there is only one way to represent a musical composition in standard musical notation. Likewise, the performance of a play springs directly from the script. For both musical and dramatic works, a change in the literal manifestation of the work has a concomitant effect on the behavioral manifestation. The same cannot be said for computer programs, because there are often numerous ways to write source code to produce a specific behavioral effect.⁵¹ Thus, limiting copyright infringement of computer programs to copying of the source code leaves the programmer with virtually no protection at all. Infringers will be permitted to copy the original programmer's work, so long as they do not copy the original source code.

C. Limitations On Protection Of Behavior

The scope of the protection for computer programs should be identical to the scope for other types of literary works. First, the dichotomy between idea and expression, fundamental to the determination of copyrightability for all types of literary works, should

49. See Margaret L. Pittman, Comment, *What The Judge Sees Is What You Get: The Implications Of Lotus v. Paperback For Software Copyright*, 37 WAYNE L. REV. 1527, 1585 (1991) (noting that limiting copyright protection for computer programs will not effectively protect the programmer's expression).

50. *Manifesto*, *supra* note 18, at 2317-18; see also FAIRLEY, *supra* note 6, at 9 (noting that an estimated 40% of the total development time of a software project is spent on analysis and design, while only 20% is typically spent on implementation (what is termed in this paper "translating the expressive design into literal source code"), debugging and unit testing); see also *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222, 1231 (3d Cir. 1986) ("[T]he coding process is a comparatively small part of programming.").

51. See *Manifesto*, *supra* note 18, at 2315-16. See also Gross, *supra* note 3, at 159 n.229 and accompanying text.

apply to program behavior. Second, the limiting doctrines of merger, *scènes à faire* and originality apply to behavior just as they do to the non-literal aspects of other literary works.

The Supreme Court opinion in the 1879 case of *Baker v. Selden*⁵² developed the modern concept of a dichotomy between idea and expression for determining copyrightability. The Court held that copyright protection for a book describing an accounting system did not extend to the actual accounting system described by the book.⁵³ The alleged infringer, Baker, had used ruled accounting sheets similar to those that had appeared in Selden's book, but had only changed the column headings and arrangement of columns. The Court concluded that the ruled accounting forms were "necessary incidents"⁵⁴ to the use of Selden's accounting system, which was "open and free to the use of the public."⁵⁵ Copyright protection was limited to Selden's particular description of the accounting system. The Court thus distinguished between the unprotectable idea expressed in Selden's book (the accounting system) and the copyrightable expression (Selden's particular description of the accounting system). The principle of *Baker* has since been codified in section 102(b) of the Copyright Act, which states that copyright protection is unavailable for any "idea, procedure, process, system, method of operation, concept, principle, or discovery."⁵⁶

In order to see how *Baker* applies to a computer program, consider the following example. Take a computer program which performs word processing functions. Assume that this word processing program includes a function which allows the printing of addresses on envelopes, a behavioral or non-literal aspect of the program. Under section 102(b), there can be no doubt that copyright protection does not extend to the "idea" of printing addresses on envelopes. Assume further that in order to print the envelopes, the word processing program must undertake the following process: (1) collect the main and return addresses from the user, (2) collect information regarding the size of the envelope from the user, (3) calculate the spacing of the addresses on the envelope, (4) send the spacing information and address information to the printer, and (5) prompt the user to place the envelope into the printer. Any word processing program that offered the function of printing an envelope would have to go through a similar, if not identical, process. Under *Baker*, therefore, this process would be uncopyrightable because it is necessarily incident to the idea of printing an envelope. Furthermore, this sequence

52. 101 U.S. 99 (1879).

53. *Id.* at 104, 107.

54. *Id.* at 103.

55. *Id.* at 101.

56. 17 U.S.C. § 102(b) (1988).

of steps would be expressly excluded from the subject matter copyrightable under section 102(b) because it would be classified as a procedure, process, system or method of operation.

While the idea of printing an envelope and the process used to perform the task are uncopyrightable, the manner in which the program implements the function and process may be considered protectable expression. This would include such things as how the user selects the function, how the program collects necessary information from the user, how the program behaves in case of an error, and so on, subject, of course, to the limiting doctrines of merger, *scènes à faire* and originality. There are multiple ways in which a program could go about performing these tasks. If multiple options for implementation exist, any specific implementation chosen by a programmer cannot be deemed necessarily incident to the idea of the function. Therefore, the particular manner by which the programmer implements the function may be considered the programmer's expression, which falls within the subject matter of copyright. Consider the explanation of this concept in *Baker*:

[T]he teachings of science and the rules and methods of useful art have their end in application and use; and this application and use are what the public derive from the publication of a book which teaches them. But as embodied and taught in a literary composition or book, their essence consists only in their statement. This alone is what is secured by the copyright. The use by another of the same methods of statement, whether words or illustrations, in a book published for teaching the art, would undoubtedly be an infringement of the copyright.⁵⁷

In the example of the envelope-addressing function, the process of printing an envelope is the useful art. The particular manner by which a program implements the function is the "statement" of this useful art, and the "use of another of the same methods of statement" (i.e., an expressive implementation that used the same or substantially similar methods) would be an infringement.⁵⁸

D. Computer Programs As Useful Articles

Objections to the protection of the behavioral aspects of computer programs often focus on the useful article doctrine because computer programs provide utility to their users.⁵⁹ The useful article doctrine of

57. *Baker*, 101 U.S. at 104.

58. See *Nimmer Declaration*, *supra* note 38, at ¶13.

59. See *Manifesto*, *supra* note 18; Leo J. Raskind, *The Uncertain Case For Special Legislation Protecting Computer Software*, 47 U. PITT. L. REV. 1131, 1143-44 (1986) (arguing that programs are uncopyrightable because of their utilitarian nature).

copyright law, articulated by the Supreme Court in *Mazer v. Stein*⁶⁰ and codified in the definition of “[p]ictorial, graphic, and sculptural work” in the current Copyright Act, states,

such works shall include works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned. The design of a useful article . . . shall be considered a pictorial, graphic, or sculptural work only if, and only to the extent that, such design incorporates . . . features that can be identified separately from, and are capable of existing independently of, the utilitarian aspects of the article.⁶¹

There are two responses to those who object to copyright protection for computer programs on the grounds that the programs are “useful articles.” First, any test for copyright infringement of a computer program which applies the limiting doctrines of traditional copyright law will filter out the purely functional aspects of the program. Only particular *implementations* of functions would be protected. Thus, fears that copyright protection for computer programs will give programmers exclusive rights to certain useful arts are unfounded.

Second, the useful article doctrine, as incorporated into the Copyright Act, does not apply to literary works, which include computer programs. The useful article doctrine often has been erroneously generalized to encompass all objects which are the subjects of copyright protection. A strict reading of the copyright statute, however, indicates that the doctrine is intended only to be applicable to pictorial, graphic, or sculptural works.⁶² The definition of these types of works, for copyright purposes, includes only those aspects of the objects which are not utilitarian, but which represent the form, or creative expression, of the creator. The categorization of a computer program as a literary work would thus seem to preclude its definition as a useful article.⁶³

Additionally, while there is no doubt that mere functions are too close to ideas to be copyrightable,⁶⁴ protection is available for sets of

60. 347 U.S. 201 (1954) (holding that statuette of a dancing figure used as a lamp base was copyrightable as a work of art despite being used in a useful object such as a lamp). “Artistic articles are protected in ‘form but not their mechanical or utilitarian aspects.’” *Id.* at 218 (citing 1909 Copyright Act, 17 U.S.C. § 202.8).

61. 17 U.S.C. § 101 (1988).

62. See Jack E. Brown, “Analytical Dissection” Of Computer Software—Complicating The Simple And Confounding The Complex, 25 ARIZ. ST. L. J. 801, 833 (1993) (discussing how the term “useful article” only appears in §§ 101 and 113 of Copyright Act, which pertain to the scope of protection for pictorial, graphic or sculptural works).

63. See *E.F. Johnson Co. v. Uniden Corp. of Am.*, 623 F. Supp. 1485, 1498 (D. Minn. 1985) (rejecting the characterization of plaintiff’s program as “a useful work” and affirming Congress’ decision to treat computer programs as “literary works:” “[T]he limitations placed on the copyrightability of useful articles by section 101 of the Act are simply not applicable here.”).

64. See *supra* part III.C.

functions as compilations. Section 103 of the Copyright Act provides protection for compilations to the extent of the expression contributed by the author,⁶⁵ even if the material that is compiled is not in and of itself copyrightable.⁶⁶ Thus, if a program provides a very unique set of functions, such that the selection of that particular set of functions represents creative expression by the programmer and is not dictated by functional considerations or constraints, then that set of functions is copyrightable. Likewise, protection should be available for compilations of behavior that implement those functions, above and beyond their inherent copyrightability. The court in the case of *Whelan Associates v. Jaslow Dental Laboratory*⁶⁷ supported this notion, noting that sequencing and ordering of materials would also be covered by copyright as compilations, "i.e., that the sequence and order could be parts of the expression, not the idea, of a work."⁶⁸

To date, few courts have used this concept to protect the behavior of programs from copying. The compilation of discrete functions or discrete elements of behavior into a single product that is useful in some way describes the essence of the creative design task of a programmer—the very thing that copyright law is meant to protect.

IV. RELEVANT CASE LAW

The courts have been uneven in their treatment of program behavior. Several courts have recognized copyright protection for some behavioral aspects of computer programs, including such elements as screen displays⁶⁹ and user interfaces.⁷⁰ Other courts have extended non-literal protection to the structure, sequence and organization of a program.⁷¹ Other courts, however, have found program behavior to fall outside the subject matter of copyright.⁷² This lack of consensus among

65. "The copyright in a compilation . . . extends only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work. . . ." 17 U.S.C. § 103(b) (1988).

66. *Miller*, *supra* note 42, at 1003. *See also supra* note 45, at §§ 3.01-04; *Harper House v. Thomas Nelson, Inc.*, 889 F.2d 197, 204-205 (9th Cir. 1989) (uncopyrightable elements of a notebook protectable as a compilation).

67. 797 F.2d 1222 (3d Cir. 1986).

68. *Id.* at 1239.

69. *See Broderbund Software v. Unison World*, 648 F. Supp. 1127, 1132 (N.D. Cal. 1986).

70. *See Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568 1576 (S.D. Fla. 1994).

71. *See Whelan*, 797 F.2d 1222, 1240 (3d Cir. 1986).

72. *See, e.g., Brown Bag Software v. Symantic Corp.*, 960 F.2d 1465 (9th Cir. 1992); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 844 (10th Cir. 1993); *Computer Assoc. Int'l. v. Altai*, 775 F. Supp. 544, 560 (E.D.N.Y. 1991), *aff'd*, 982 D.2d 693 (2nd Cir. 1992).

the courts has led to confusion over the protectability of program behavior.

The courts that have upheld copyright protection for behavioral elements of programs have taken notice of the fact that behavior represents the programmer's expression. These courts have realized that behavioral elements are "as valuable, if not more valuable, than the program code and structure itself and, therefore, warrant protection."⁷³ For example, in *Lotus Development Corp. v. Paperback Software International*,⁷⁴ the court expressed concern that if the scope of protection for computer programs is too narrow, "copyright law never would, as a practical matter, provide computer programs with protection as substantial as Congress has mandated—protection designed to extend to original elements of expression *however embodied*."⁷⁵

In *Whelan Associates v. Jaslow Dental Laboratory*,⁷⁶ the Third Circuit took an important first step toward recognition of the behavioral aspects of programs. The court noted that other literary works could be infringed through non-literal copying, citing the example that "[o]ne can violate the copyright of a play or book by copying its plot or plot devices."⁷⁷ The court then drew the conclusion by analogy that the copyright of a program could be infringed "even absent copying of the literal elements of the program."⁷⁸ The court made its analysis within the framework of the traditional idea/expression dichotomy of *Baker* and section 102(b) of the Copyright Act, deciding that the idea expressed by the programmer was the function of the program, with the actual program being the programmer's expression of that idea.⁷⁹ The court reasoned that since there were a variety of ways in which the program could have been implemented, "the [dynamic] structure is not a necessary incident to that idea,"⁸⁰ and was therefore copyrightable expression. The court also relied on public policy to reach this conclusion, noting that "we must remember that the purpose of the copyright law is to create the most efficient and productive balance between protection (incentive) and dissemination of information, to promote learning, culture and development."⁸¹

73. John Houston, Comment, *A Unified Test For The Copyright Protection Of The User Interface To Computer Programs*, 32 DUQ. L. REV. 133, 142 (1993).

74. 740 F. Supp. 37 (D. Mass. 1990).

75. *Id.* at 56 (emphasis added).

76. 797 F.2d 1222 (3d Cir. 1986).

77. *Id.* at 1234.

78. *Id.*

79. *Id.* at 1238-40.

80. *Id.* at 1240.

81. *Id.* at 1235.

While the *Whelan* court has been widely criticized for providing over-broad protection for programs, the court nonetheless correctly concluded that the non-literal aspects of a program are protectable under copyright.⁸² *Whelan* provides the basis for an argument that non-literal aspects of a program—in other words, the program behavior—are copyrightable.

Though the courts continue to disagree over the proper scope of copyright protection for computer programs, most courts appear to agree upon the Abstraction-Filtration-Comparison (AFC) test, formulated in *Computer Associates International v. Altai, Inc.*,⁸³ as the proper test for non-literal infringement of computer programs. The Second Circuit's AFC test has been adopted in some form by the Fifth Circuit,⁸⁴ the Ninth Circuit,⁸⁵ the Tenth Circuit,⁸⁶ the Federal Circuit,⁸⁷ and by district courts in the Eleventh Circuit.⁸⁸

The district court in *Altai* expressly took notice of the bifurcated nature of the programmer's expression in computer programs:

Each view—textual and behavioral—has its own structure, sequence, and organization. In the standard jargon of programmers, there is static structure, which refers to the program-as-text view, and dynamic structure, which refers to the program-as-behavior view. The static structure and dynamic structure of a program can be quite different; indeed from dealing with the behavior of a program, i.e., operating it, one can tell virtually nothing about its text. Thus . . . "it makes no technical sense to talk simply about the 'structure' of a program, because the term is ambiguous and the distinction [between dynamic structure and static structure] matters."⁸⁹

82. See, e.g., Englund, *supra* note 40; Michael A. Jacobs, *Copyright and Compatibility*, 30 JURI. J. 91 (1989); Andrew O. Martyniuk, Comment, *Abstraction-Filtration-Comparison Analysis and the Narrowing Scope of Copyright Protection for Computer Programs*, 63 U. CIN. L. REV. 1333 (1995); Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045 (1989); Pamela Samuelson, *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, 6 HIGH TECH. L. J. 209 (1991); Peter G. Spivak, Comment, *Does Form Follow Function? The Idea/Expression Dichotomy in Copyright Protection of Computer Programs*, 35 UCLA L. REV. 723 (1988); Nicholas P. Terry, *GUI Wars: The Windows Litigation and the Continuing Decline of "Look And Feel"*, 47 ARK. L. REV. 93, 142, n.222-24 (1994).

83. 775 F. Supp. 544 (E.D.N.Y. 1991), *aff'd in part, vacated in part, remanded*, 982 F.2d 693 (2d Cir. 1992).

84. *Engineering Dynamics v. Structural Software, Inc.*, 26 F.3d 1335, 1342-43 (5th Cir. 1994); *Kepner-Tregoe, Inc. v. Leadership Software, Inc.*, 12 F.3d 527, 536-37 (5th Cir. 1994).

85. *Apple Computer v. Microsoft Corp.*, 35 F.3d 1435, 1442-43 (9th Cir. 1994).

86. *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 834 (10th Cir. 1993); *Autoskill v. Nat. Educ. Support Sys.*, 994 F.2d 1476, 1487-98 (10th Cir. 1993).

87. *Atari Games Corp. v. Nintendo of Am.*, 975 F.2d 832, 839 (Fed. Cir. 1992).

88. *Mitek Holdings v. Arce Eng'g Co.*, 864 F. Supp. 1568, 1577-78 (M.D. Fla. 1994); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337, 352-54 (M.D. Ga. 1992).

89. *Altai*, 775 F. Supp. at 559-60.

The *Altai* court criticized *Whelan* as being "inadequate and inaccurate" for ignoring the distinction between the static and dynamic structure of a program, and for assuming that a program is the expression of a single idea, instead of the expression of multiple ideas.⁹⁰

The *Altai* court, however, wrongly expressed doubts as to the copyrightability of a program's "dynamic structure"—in other words, the behavioral manifestation of the program. The *Altai* court's misgivings over the protectability of program behavior stemmed from its misinterpretation of section 102(b) of the Copyright Act.⁹¹ The district court stated that "since the behavior aspect of a computer program falls within the statutory terms 'process,' 'system,' and 'method of operation,' it may be excluded by statute from copyright protection."⁹² Yet, the court stopped short of holding as a matter of law that program behavior was a system, process or method of operation, thereby leaving the door open for copyright protection of program behavior. The *Altai* court held that the plaintiff's rights were fully protected by examining the literal program code, thus permitting the court to avoid determining whether program behavior should be excluded from the subject matter of copyright.⁹³ Thus the district court left the issue of the protectability of program behavior for another court, or for Congress, to decide.

In affirming the district court in *Altai*, the Second Circuit panel devised the three-step AFC test⁹⁴ for determining infringement of computer programs based on the abstraction test devised by Judge Learned Hand in the case of *Nichols v. Universal Pictures*,⁹⁵ which involved a non-literal infringement claim by an author of a play against the producer of another play. The AFC test applies concepts of traditional copyright law such as the idea/expression dichotomy and the limiting doctrines of merger, *scènes à faire* and originality to computer programs. As such, it is seen by many as a narrowing of the protection for non-literal aspects of computer programs after *Whelan*.⁹⁶ Nonetheless, *Altai* affirms that traditional copyright law principles are applicable to the non-literal aspects of computer programs. *Altai's* AFC test also provides an appropriate framework upon which a test for infringement can be built.

90. *Id.* at 559.

91. "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work." 17 U.S.C. § 102(b) (1988).

92. *Altai*, 775 F. Supp. 544 at 560.

93. *Id.*

94. See *infra* part VI.

95. 45 F. 2d 119, 121 (2d Cir. 1930).

96. See *supra* note 68 and accompanying text.

The behavior-based test proposed in this article is a modification of the AFC test.⁹⁷

Since *Altai*, several other courts have upheld protection for non-literal behavioral aspects of computer programs.⁹⁸ In the case of *Autoskill v. National Educational Support Systems*,⁹⁹ the Tenth Circuit applied the *Altai* test and determined that a program implementing a reading system was infringed by another program which simply changed the names and sequences of tests in the operation of the infringing program. In *Mitek Holdings v. Arce Engineering Co.*,¹⁰⁰ the district court, in applying the *Altai* test, determined that some non-literal, behavioral elements of the allegedly infringed program were protectable.¹⁰¹ The court concluded, however, that there was not enough similarity to make a finding of infringement.¹⁰² Though the court found no infringement, the significance of *Mitek* lies in the court's recognition that some behavioral elements were found to be protectable.

In *Apple Computer v. Microsoft*,¹⁰³ the Ninth Circuit identified similarities between discrete behavioral elements in both the copyrighted and allegedly infringing programs.¹⁰⁴ The Ninth Circuit, however, held there was no infringement because most of the similarities were permitted by a license agreement between the plaintiff and the defendant, or were obvious expressions of basic ideas, and thus precluded from copyright protection by the merger doctrine.¹⁰⁵ As such, the court felt that infringement could only be found if the works as a whole were virtually identical.¹⁰⁶ This case provides yet another example of an instance where a court has embraced the notion that behavioral elements of a program are protectable, though infringement was not found.

Other courts, however, have followed the dicta in *Altai*, concluding that protection from non-literal infringement does not extend to program behavior. In *Gates Rubber Co. v. Bando American, Inc.*,¹⁰⁷ the district court explicitly held that the behavior of a computer program was protectable:

The court will respectfully disagree with the *Altai* decision and hold that a program's behavior can be protected by copyright law [T]he

97. See *infra* part VI.

98. See *supra* note 7.

99. 994 F.2d 1476 (10th Cir. 1993).

100. 864 F. Supp. 1568 (S.D. Fla. 1994).

101. *Id.* at 1577-78.

102. *Id.* at 1580.

103. 35 F.3d 1435 (9th Cir. 1994).

104. *Id.* at 1438.

105. *Id.* at 1446.

106. *Id.* at 1447.

107. 798 F. Supp. 1499 (D. Colo. 1992), *vacated and remanded in part, aff'd in part*, 9 F.3d 823 (10th Cir. 1993).

commonality of [the] error denotes "behavior" as to how one part of the program works with another. This is *part of the creative expression* of the program itself.¹⁰⁸

The Tenth Circuit reversed, however, holding that the district court had failed to properly eliminate the behavioral elements of the program from the determination of infringement.¹⁰⁹

The First Circuit decision in the case of *Lotus Development Corp. v. Borland International*¹¹⁰ further confused the issue of protectability of behavior. The First Circuit, in reversing the district court's finding that the menu command structure of the plaintiff's program was protectable, held that menu command structure was a "method of operation" and therefore uncopyrightable under section 102(b).¹¹¹ The court stated that the *Altai* test was applicable to non-literal copying, but that the appropriation of the menu command structure represented literal copying, and thus the *Altai* test did not apply.¹¹² What the court failed to take into account, however, was that the literally copied portion of the program was in reality a non-literal behavioral aspect of the program.

Given the uneven treatment by the courts, the protectability of behavioral aspects of programs remains uncertain. Much of the difficulty lies in agreeing upon the common terminology to describe literal and non-literal aspects of a program. The disagreement, however, appears ripe for a decision by the Supreme Court.¹¹³

V. THE PROPOSED BEHAVIOR-BASED TEST

The test advocated by this article would look solely at the behavioral manifestation of the programmer's expression and would ignore the literal manifestation when determining whether infringement has occurred.¹¹⁴ Once the behavioral elements have been isolated, the proposed behavior-based test would apply the idea/expression dichotomy and traditional copyright limiting doctrines such as merger, *scènes a faire* and originality to determine which behavioral elements deserve copyright protection and which elements ought to be excluded. The behavioral elements of the original work would then be compared

108. *Id.* at 1518-19 (emphasis added).

109. 9 F.3d 823 at 835.

110. 49 F.3d 807 (1st Cir. 1995).

111. *Id.* at 815.

112. *Id.* at 814.

113. The Supreme Court has granted a writ of certiorari in the *Lotus* case. *Lotus Dev. Corp. v. Borland Int'l*, 116 S.Ct. 39 (1995).

114. If a program is literally copied (i.e. the source code of the program is duplicated) then the behavior of the copy would be identical to the behavior of the original, and would thus infringe under this test.

with the behavioral elements of the infringing program to determine whether there is substantial similarity between them. A test of this nature makes more sense in light of the nature and realities of computer programs and the public policy surrounding traditional copyright law.

A good starting point for defining such a test is the AFC test articulated by the Second Circuit in *Computer Associates International, v. Altai, Inc.*¹¹⁵ This test has been adopted, in one form or another, by several courts in cases involving infringement of non-literal aspects of computer programs.¹¹⁶ The *Altai* test consists of a three-step procedure which is used to determine if an allegedly infringing program is substantially similar to the allegedly infringed program.

In ascertaining substantial similarity under this approach, a court would first break down the allegedly infringed program into its constituent structural parts. Then, by examining each of these parts for such things as incorporated ideas, expression that is necessarily incidental to those ideas, and elements that are taken from the public domain, a court would then be able to sift out all non-protectable material. Left with a kernel, or possible kernels, of creative expression after following this process of elimination, the court's last step would be to compare this material with the structure of an allegedly infringing program. The result of this comparison will determine whether the protectable elements of the programs at issue are substantially similar so as to warrant a finding of infringement.¹¹⁷

1. ABSTRACTION

The abstraction step, described above as "break[ing] down the allegedly infringed program into its constituent structural parts," requires the court to reconstruct the programmer's implementation of the program in reverse order.

115. 982 F.2d 693, 706-711 (2d Cir. 1992).

116. See, e.g., *Lotus Dev. Corp. v. Borland Int'l*, 49 F.3d 807, 816 (1st Cir. 1995), cert. granted, 116 S.Ct. 39 (1995) ("*Altai* test may provide a useful framework for assessing the alleged nonliteral copying of computer code."); *Lotus Dev. Corp. v. Borland, Int'l.*, 799 F. Supp. 203 (D. Mass. 1992) (concluding that the test developed by the district court was "compatible substantively, though different in methodology" than the *Altai* test); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 828 (10th Cir. 1993) ("In substantial part, we adopt the 'Abstraction-Filtration-Comparison' test."); *Productivity Software Int'l. v. Healthcare Tech.*, 1995 WL 437526 (S.D.N.Y. 1995) (using *Altai* test to determine substantial similarity); *Triad Sys. Corp. v. Southeastern Express Co.*, 31 U.S.P.Q.2d (BNA) 1239, 1248 (N.D. Cal. 1994) (using first two steps of the *Altai* test for distinguishing between protectable expression and unprotectable ideas, processes, etc., where substantial similarity was not disputed); *Atari Games Corp. v. Nintendo of Am., Inc.*, 30 U.S.P.Q.2d 1401 (BNA) (N.D. Cal. 1993) ("In our view, in light of the essentially utilitarian nature of computer programs, the Second Circuit's approach is an appropriate one.").

117. *Altai*, 982 F.2d at 706.

Initially, in a manner that resembles reverse engineering on a theoretical plane, a court should dissect the allegedly copied program's structure and isolate each level of abstraction contained within it. This process begins with the code and ends with an articulation of the program's ultimate function. Along the way, it is necessary essentially to retrace and map each of the designer's steps—in the opposite order in which they were taken during the program's creation.¹¹⁸

This step of the test requires that the court acquire knowledge equivalent to that of a computer program developer, a requirement which is beyond the capability of most courts. As a result, expert analysis and testimony is usually required to assist the court in performing the abstraction step of the test.

The proposed behavior-based test would eliminate the abstraction step of the *Altai* test. The first step of the test would instead involve identifying the discrete elements which represent the program's behavior. Call this the "identification" step. The court should identify the behavioral elements of a computer program simply by operating the program on a computer. This will permit observation of how the program behaves. For example: "the program performs functions X, Y and Z" or "when the user does this, the program responds by doing that." The level of complexity of the observations is a function of the complexity of the program. For a more complicated program, instead of observing "when the user does this, the program does that," it may be necessary to observe that "when the user does this, and conditions A, B and C are met, then the program does that."

As an example, it may be helpful to consider the small icon resembling a trash-can which appears on the lower right hand corner of the Apple Macintosh user interface. When a user uses the mouse to drag a file icon into the trash-can icon, the file icon is prepared for deletion from the computer's disk. This description of the trash-can icon and its function identifies a certain behavioral element of the program which generates the user interface of the Apple Macintosh. Thus, the first step of the behavior-based test has been completed.

2. FILTRATION

The second step of the *Altai* test, the filtration step, requires the court to apply traditional limiting doctrines of copyright law to the abstractions formulated in the first step of the test. It is described as "examining each of these parts for such things as incorporated ideas, expression that is necessarily incidental to those ideas, and elements that are taken from the public domain." In essence, the court is to apply the

118. *Id.* at 707.

doctrines of merger, *scénès a faire* and originality to the various levels of abstraction.

This process entails examining the structural components at each level of abstraction to determine whether their particular inclusion at that level was an "idea" or was dictated by considerations of efficiency, so as to be necessarily incident to that idea [merger doctrine]; required by factors external to the program itself [*scénès a faire* doctrine]; or taken from the public domain [originality requirement] and hence is nonprotectable expression.¹¹⁹

The purpose of this test is to "filter out" subject matter that is unprotectable. After the application of this step of the test, the fact finder is left with the protectable expression of the allegedly infringed program.

The *Altai* court first applied the merger doctrine to the abstracted structure of the program. The principle underlying the merger doctrine was well-stated by the First Circuit in the *Concrete Machinery Co. v. Classic Lawn Ornaments, Inc.*¹²⁰ The court stated, "[w]hen there is essentially only one way to express an idea, the idea and its expression are inseparable and copyright is no bar to copying that expression."¹²¹ The *Altai* court also applied this doctrine to computer programs, stating, "[i]n the computer context, this means that when specific instructions, even though previously copyrighted, are the only and essential means of accomplishing a given task, their later use by another will not amount to infringement."¹²²

The proposed behavior-based test would apply the merger doctrine as stated in *Concrete Machinery* to the behavioral elements of the program which were observed in the identification step of the test. Continuing with the above example of the Apple Macintosh trash-can icon, one can imagine an almost infinite number of ways in which the function which deletes a file from the computer's disk could be implemented. The trash-can icon is therefore not rendered unprotectable by the merger doctrine.

The *Altai* court then applied the "*scénès a faire*" doctrine. This doctrine states that when external factors constrict the possible ways to express an idea, such expression is not protectable by copyright. Professor Nimmer, in his treatise on copyright law, has identified five instances of external factors which may circumscribe the manner in which a program is designed.¹²³ The *Altai* court adopted these factors.¹²⁴ They are: (1) the mechanical specifications of the computer on which a particular program

119. *Id.*

120. 843 F.2d 600 (1st Cir. 1988).

121. *Id.* at 606.

122. *Altai*, 982 F.2d at 708.

123. 3 NIMMER & NIMMER, *supra* note 45, at 13-65.

124. *Altai*, 982 F.2d at 709.

is intended to run; (2) compatibility requirements of other programs with which a program is designed to operate in conjunction; (3) computer manufacturer's design standards; (4) demands of the industry being serviced; and (5) widely accepted practices within the computer industry.¹²⁵

The proposed behavior-based test adopts these factors as well, but applies them to the observations of the identification step of the test, instead of to the level of structural abstractions identified in the abstractions step of the *Altai* test. In the example of the trash-can icon, it is unlikely that any of the five factors listed above would require that a user interface allow users to delete files from the computer's disk in this fashion.

Finally, the *Altai* court applied the originality standard to the levels of abstraction. This limitation is based on the statutory requirement that copyright protect only "original works of authorship."¹²⁶ In the context of a computer program, this excludes from protection material which is taken from the public domain. The *Altai* court stated, "Such material is free for the taking and cannot be appropriated by a single author even though it is included in a copyrighted work."¹²⁷

The proposed behavior-based test also adopts this standard, as applied to the discrete behavioral elements of the program observed in the identification step of the test. Returning yet again to the trash-can icon example, assuming that Apple is the originator of this particular feature, its copyrightability would be unaffected by the filtration step of the test.

3. COMPARISON

The final step of the *Altai* test is the comparison step. The court described this step of the test as, "whether the defendant copied any aspect of this protected expression, as well as an assessment of the copied portion's relative importance with respect to the plaintiff's overall program."¹²⁸

The proposed behavior-based test also includes this step of the *Altai* test. The discrete behavioral elements of the alleged infringing program are to be compared with the discrete behavioral elements of the allegedly infringed program which are copyrightable, i.e., those that remain after the filtration step. The comparison should be performed both in terms of quantity and quality of copying. In other words, if the infringing program copied substantial portions of the original program, then a finding of

125. *Id.*

126. 17 U.S.C. § 102(a) (1988).

127. *Altai*, 982 F.2d at 710.

128. *Id.* at 710.

infringement is warranted. Likewise, if only a small portion has been copied but the portion copied is qualitatively substantial, that is, the particular behavior copied makes the original program particularly valuable and desirable to consumers, then a finding of infringement may also be warranted.

VI. AN APPLICATION OF THE PROPOSED BEHAVIOR-BASED TEST

To illustrate how the proposed behavior-based "Identification-Filtration-Comparison" test operates, it may be useful to look at its application to a real case. The case of *Lotus Development Corp. v. Borland International*¹²⁹ provides a good opportunity to examine behavioral elements of a computer program.

The dispute in the case arose when Borland copied portions of the Lotus 1-2-3 spreadsheet program in its own spreadsheet product. Specifically, Borland included in its product a mode which emulated the menu command structure of 1-2-3. The menu command structure is the part of the user interface of the program which allows users to input commands to the program.¹³⁰ Additionally, the 1-2-3 menu command structure also facilitated the running of 1-2-3 user-written macros.¹³¹ The Borland spreadsheet product permitted its users to operate the program in a mode which copied the 1-2-3 menu command structure. This served two purposes. First, it allowed users who were familiar with the 1-2-3 menu command structure to easily switch to the Borland product. Secondly, it allowed users who had written macros for 1-2-3 to run those macros from within the Borland product. The Borland product also featured a "Key Reader" facility which allowed the running of the 1-2-3

129. 788 F. Supp. 78 (D. Mass. 1992), 799 F. Supp. 203 (D. Mass. 1992), 831 F. Supp. 202 (D. Mass. 1992), 831 F. Supp. 223 (D. Mass. 1992), *rev'd.*, 49 F.3d 807 (1st Cir. 1995), *cert. granted*, 116 S.Ct. 39 (1995).

130. A menu is a list of command options available to the user of a program. See WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 365. The menu command structure of 1-2-3 consists of a series of commands, spaced horizontally across the top of the screen, from which the user can select, using the computer's mouse or keyboard. These commands are the top of a tree of commands available to the user. When one of these commands is selected, a sub-menu of commands, or another branch in the tree of commands, appears. Each item in the sub-menu that the user could select is either another branch in the tree of commands, leading to another sub-menu, or a leaf of the tree, representing a command which tells the program to perform a specific function.

131. A macro is a single command, made up by a user, which can replace a series of the 1-2-3 commands. A user can define a series of 1-2-3 commands, and assign a name to the series. This "macro" can then be invoked by using the assigned name, instead of having to enter each 1-2-3 command in the series individually. See WEBSTER'S DICTIONARY OF COMPUTER TERMS, *supra* note 14, at 351.

macros even when the 1-2-3 menu command structure was not being used.

The district court in the case found that the Borland product infringed the 1-2-3 product. To make this determination, the court used a test which it claimed was compatible with the *Altai* Abstraction-Filtration-Comparison test.¹³² The First Circuit Court of Appeals subsequently overturned this decision, stating that the 1-2-3 menu command structure was a "method of operation" and was thereby uncopyrightable under the copyright statute.¹³³ The Supreme Court has since granted certiorari on the case.¹³⁴

In applying the "Identification-Filtration-Comparison" test outlined above, the first step is to observe the behavior of the program and identify its behavioral elements. There is no doubt that the operation of the menu command hierarchy is a behavioral element, or several behavioral elements of the 1-2-3 program. When a user selects any item in any sub-menu, the 1-2-3 program responds with a specific response, either the posting of a new sub-menu, or the invocation of a program function. In a complete analysis of the case, the court would be required to identify all of the behavioral elements of the program, including the layouts of the screens, the manner in which the functions of the program are carried out, how error messages are posted, etc. For purposes of this example, however, we will stop at the observation that the menu command structure represents a set of discrete behavioral elements of the 1-2-3 program which, if not filtered out by the next step of the test, are copyrightable as the expression of the programmer.

The filtration step of the test determines if any of the behavioral elements observed in the identification step of the test should be rendered unprotectable because of the application of one of the limiting doctrines of copyright law. It does not appear that there is any merger of idea and expression with regard to the menu command structure. The manner in which the Lotus designers implemented the menu command structure of 1-2-3 is certainly not the only way that it could be done. The existence of the alternate method used by the Borland product proves this. Likewise, we will assume that the design of the 1-2-3 menu command structure was original to the Lotus designers.

The application of the *scènes à faire* doctrine, however, raises issues as to the copyrightability of the menu command structure. One of the factors identified by Nimmer and adopted by the *Altai* court was "compatibility requirements of other programs with which a program is

132. *Lotus*, 799 F. Supp. at 223-23, 831 F. Supp. at 245.

133. *Lotus*, 49 F.3d at 815.

134. *Lotus*, 116 S.Ct. 39 (1995).

designed to operate in conjunction." In this case, the Borland program wishes to allow its users to run the macros they have created using the 1-2-3 program. There is no way to allow the running of the 1-2-3 macros without the menu command structure being recreated in one form or another. The copying of the menu command structure represents a design constraint of making the Borland product compatible with the 1-2-3 program. Thus, the discrete behavioral elements making up the 1-2-3 menu command structure must be filtered out from the set of protectable behavioral elements of the 1-2-3 program.

The application of the comparison step of the test is moot at this point because all of the behavioral elements which have been copied by the alleged infringing Borland program have been filtered out of the set of copyrightable behavioral elements of the 1-2-3 program. Thus, there can be no infringement.

VII. CONCLUSION

Some commentators have argued that protection for computer programs would be better provided under patent law¹³⁵ or a sui generis intellectual property regime.¹³⁶ This article, however, suggests that copyright law is flexible enough to accommodate new creative works like computer programs by applying traditional copyright doctrines and weighing modern public policy objectives. Furthermore, a copyright regime that denies a programmer protection from copying of the behavioral aspects of his programs is tantamount to providing him no protection whatsoever. This article has presented several arguments why such protection is necessary and suggested a method by which courts may properly carry out the congressional mandate to extend copyright protection to computer programs.

135. Mark A. Lemley, *Convergence in the Law of Software Copyright*, 10 HIGH TECH. L.J. 1 at 26 (1995) ("Altering copyright law rather than employing patent protection has arguably overprotected computer software . . .").

136. See generally *Manifesto*, *supra* note 18.

BOOK REVIEW

DNA IN THE COURTROOM: A TRIAL WATCHER'S GUIDE

**by HOWARD C. COLEMAN & ERIC D. SWENSON
GENELEX PRESS, SEATTLE, WA; 131 PAGES; \$12.95**

REVIEWED BY JASMINE SAMRAD[†]

Scientific technologies have expanded exponentially in our century, leaving virtually no aspect of our lives unaffected. Nowhere is this more obvious than in our courtrooms, which have turned into science battlegrounds where ever more complex technologies are introduced as evidence. These new technologies challenge us not only to grasp their scientific complexity but also to evaluate their reliability as evidence. One of the seminal challenges in the field of scientific evidence has been the struggle to assimilate the revolutionary new DNA technologies, especially DNA fingerprinting, into the legal system. Nevertheless, until the O.J. Simpson trial drew the nation's attention to the controversy, few people outside the relevant legal and scientific fields were aware of its scope and significance.

The much-publicized battle between Simpson's defense team and prosecutors regarding DNA evidence was, however, only a relatively minor skirmish in an ongoing "DNA War" over the introduction of this revolutionary forensic technology into our courtrooms. Since soon after the technique's discovery in 1985, proponents of DNA fingerprinting have battled critics who questioned the reliability of the technique, the interpretation of results and their admissibility in criminal trials. Many of the criticisms initially raised, such as proper testing procedures and statistical analysis methods, have since been addressed or refuted, and the technology has gathered widening support in the scientific community. Nevertheless, some critics have persisted in their attacks, perpetuating the confusion and controversy. The debates have highlighted not only the complexities of DNA

© 1995 Jasmine Samrad.

[†] J.S.D. Candidate, 1997, LL.M., 1995, Boalt Hall School of Law, University of California, Berkeley. J.D., School of Law, 1993, B.S., 1989, University of California, Davis.

fingerprinting evidence, but also the difficulty of incorporating scientific evidence into our present judicial structure.

*DNA in the Courtroom: A Trial Watcher's Guide*¹ by Howard Coleman and Eric Swenson is a handy primer on the DNA controversy, covering the technology of DNA fingerprinting and the legal treatment of DNA evidence. Coleman is president of GeneLex Corporation, a nationally recognized laboratory that performs DNA testing for both forensic analysis and determination of parentage.² Swenson is a professional writer and teacher of technical writing. The collaboration of these two authors results in a thorough, technically accurate yet eminently readable work that will be of interest to a broad audience. The book's original purpose, to provide a technical guide for reporters covering the Simpson trial, evidences itself in the lucidity and accessibility of its presentation. The work is a welcome resource in this highly charged area of both scientific and legal complexity. Although the book is especially appropriate for those with no scientific or legal background who need a clear and concise introduction to DNA fingerprinting, the book is comprehensive enough to offer insights even to those with strong knowledge in the field.

SYNOPSIS

DNA in the Courtroom: A Trial Watcher's Guide contains six short chapters that provide a historical account of the major battles in the DNA war, explain the science and technology of forensic DNA fingerprinting and discuss treatment of DNA under the law of scientific evidence. The book includes a chapter specifically on the Simpson trial, which is not as superfluous as one might think even at this late date, and a useful appendix listing the status of DNA fingerprinting in forty-seven states with relevant case law.

Chapter One chronicles the major battles of the DNA controversy and is one of the most intriguing and entertaining sections of the book. Coleman, himself a DNA expert with extensive experience testifying and teaching about forensic and parentage DNA testing, provides a blow-by-blow, front-line view of the DNA controversy. His account mirrors other reports³ in portraying the

1. HOWARD C. COLEMAN & ERIC D. SWENSON, *DNA IN THE COURTROOM: A TRIAL WATCHER'S GUIDE* (1994).

2. Determination of paternity, maternity, or other kinship is referred to as "parentage testing."

3. See, e.g., William C. Thompson, *Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War,"* 84 J. CRIM. L. & CRIMINOLOGY 22, 100-03 (1993).

controversy as unusually acrimonious, with both proponents and opponents of DNA evidence often resorting to attacking the qualifications and the character of opposing experts, rather than attacking the evidence itself. Coleman attributes the contentiousness of the DNA fingerprinting controversy to several factors: the commercial motives of the labs that developed the technologies, the "contentious and fragmented nature of our legal system," and inaccurate media coverage.⁴

The introduction of this revolutionary technology into the courtroom by private companies, an element unique in the history of forensic science, played a key role in creating and perpetuating the controversy. These companies' pursuit of commercial goals created an environment unfavorable to the introduction of a technology with such vast potential for changing the criminal justice system.⁵ The major private laboratories were engaged in a race to the courtroom, attempting to license their procedures and sell their products to as many forensic laboratories as possible.⁶ The companies strove to gain a competitive advantage by keeping their products and technologies secret.⁷ The normal procedures for validating new scientific methods, such as publication, peer review and standardization, were bypassed in the commercial laboratories' rush to get a return on their substantial investment and start-up costs.⁸ Moreover, companies used different tools and procedures, which precluded easy comparison of results between companies.⁹

This commercially competitive climate delayed the development of adequate quality control and validity standards.¹⁰ Meanwhile the private companies, aided by "an adulatory press," avidly promoted the new technology to the bench, the bar and law enforcement.¹¹ Thus DNA fingerprinting initially enjoyed a nearly meteoric rise to stardom in the forensic science landscape. Courts and commentators almost universally accepted and hailed DNA fingerprinting as a reliable and accurate identification tool that promised to revolutionize the criminal justice system.¹² A stunned

4. COLEMAN & SWENSON, *supra* note 1, at 1.

5. *Id.* at 4.

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *See id.* at 5.

11. *Id.*

12. *See id.* *See also* THOMPSON, *supra* note 3, at 22; ANDRE A. MOENSSSENS ET AL., SCIENTIFIC EVIDENCE IN CIVIL AND CRIMINAL CASES 938 (4th ed. 1995).

defense bar, caught unawares, made few objections and viewed the new technology as virtually impossible to defend against.¹³ Soon, however, defense attorneys rallied and delivered their first major victory against the admissibility of DNA fingerprints in the landmark case *People v. Castro*.¹⁴ Thus began the so-called "DNA Wars."

Coleman and Swenson deliver a succinct summary of *Castro* and the major arguments propounded against admitting the DNA fingerprinting evidence. Jose Castro was charged with the murder of a pregnant women and her daughter after DNA from blood found on Castro's watch was found to match the woman's DNA. The trial court in *Castro* excluded the DNA evidence inculpatory Castro after experts from both the prosecution and defense testified that the DNA fingerprints were obtained under flawed conditions and were therefore unreliable.¹⁵ No appellate opinion on whether flawed DNA testing conditions preclude admissibility ever materialized since, soon after the DNA evidence was excluded, Castro confessed to the crime and pled guilty.¹⁶ Nevertheless, *Castro's* impact remained substantial; DNA evidence and the laboratories that performed them could no longer be viewed as infallible.

Castro was the spark igniting the powder keg of controversy that became known as the "DNA Wars." *DNA in the Courtroom* describes the DNA battles as they were fought in the courts, in academic circles and in the media, where the press had a field day bashing the technology it had previously called a miracle.

Coleman and Swenson claim the media fueled the DNA controversy through sensational, misleading or downright inaccurate reporting.¹⁷ One example comes from the *New York Times's* coverage of

13. COLEMAN & SWENSON, *supra* note 1, at 5.

14. 144 Misc. 2d 956 (N.Y. 1989).

15. See COLEMAN & SWENSON, *supra* note 1, at 6. The court found that the theories underlying DNA fingerprinting were reliable enough to render DNA evidence generally admissible, but that inaccuracies in performance of the tests rendered these particular match results too unreliable to be admitted. These inaccuracies included the laboratory's apparent inculpatory bias when drawing conclusions from ambiguous data, failure to use adequate controls to verify that interpretations were correct, ignoring the failure of some controls that were used, THOMPSON, *supra* note 3, at 43, and failure to adequately correct for bacterial contamination, Thomas M. Fleming, Annotation, *Admissibility of DNA Identification Evidence*, 84 A.L.R. 4th 313, 331-32 n.56 (1991). Courts today continue to split over the significance of proper performance of testing procedures. Some hold that performance of the technique goes to the weight, rather than the admissibility, of the test results, while other courts require proper performance of tests before the DNA evidence can be admitted. MOENSENS, *supra* note 12, at 942-43.

16. COLEMAN & SWENSON, *supra* note 1, at 6.

17. See *id.* at 13-14.

the important National Research Council report, *DNA Technology in Forensic Science*.¹⁸ The report explicitly recommended the *continued use* of DNA fingerprints in court, emphasizing only the need to apply adequate quality control protocols and recommending a conservative (pro-defendant) method of statistical analysis.¹⁹ However, the *Times* completely misrepresented the report's findings as advocating a *ban* on DNA evidence until the scientific basis was stronger.²⁰

In addition to irresponsible media coverage and the commercial interests of the private companies, other elements also played a role in perpetuating the confusion and controversy regarding DNA fingerprints. The authors mention as exacerbating factors the strategies and politics of both the prosecution and defense bar,²¹ and the expert witnesses who often have a vested interest in perpetuating the controversy so their services will still be needed.²² The authors plainly believe that the DNA controversy was largely overblown and unnecessarily exacerbated by all of these factors. However, one of the book's weaknesses is its failure to acknowledge the benefits resulting from the controversy. The authors do seem to concede that focusing national attention on the importance of standardization and quality control did provide some gains. For example, the authors note that the FBI's creation of a national DNA laboratory caused the "standardization of a chaotic industry."²³ However, they fail to analyze the possible connection between the rising tide of criticism against DNA fingerprints, defense victories like *Castro* and the development of such national DNA laboratories.

Coleman and Swenson expressly state in their preface that they are strong proponents of admitting DNA evidence. Perhaps because of this perspective, the general tone of the book seems to blame the perpetuation of the controversy largely on the defense bar and its experts. The authors seem to suggest that the defense bar sometimes went beyond proper zealous advocacy to the point of intentionally muddying the waters and confusing the issues. If this is their view,

18. *Id.*

19. *Id.* See generally COMMITTEE ON DNA TECHNOLOGY IN FORENSIC SCIENCE, NATIONAL RESEARCH COUNCIL, *DNA TECHNOLOGY IN FORENSIC SCIENCE* (1992).

20. COLEMAN & SWENSON, *supra* note 1, at 13.

21. See *id.* at 16-18. The authors also argue that the DNA controversy has been exacerbated by a "politicization" of the judicial process, where prosecutors "adopt a bunker mentality when under attack while doing their job of protecting us from criminals, [while defense attorneys] feel under siege because they usually have even fewer resources. . . . than does the prosecution" and must fulfill their role of safeguarding individual liberties. *Id.* at 16-17.

22. *Id.* at 18.

23. *Id.* at 7.

they are by no means alone. Nonetheless, the authors make an obvious attempt to present a balanced view, identifying errors by all involved parties, including the prosecution, the media, the judiciary and the scientific community.

The remaining chapters of the book describe the science behind DNA fingerprinting and the use of DNA evidence in the courtroom. In chapters Two and Three, the authors provide an explanation of the theory and practice of DNA fingerprinting; these two chapters are exemplary in their thoroughness and accessibility. Readers need no scientific literacy whatsoever to grasp the explanations offered here. The authors supplement their descriptions with helpful lay analogies and extremely useful charts and diagrams.

Chapter Two describes DNA evidence as a tool in the field of forensic serology, explaining the possible sources of DNA, such as blood, semen, or hair roots,²⁴ and comparing DNA typing with the other major types of serological evidence such as traditional blood typing and human leukocyte antigen (HLA) analysis. DNA evidence presents several advantages over traditional types of blood analysis. For example, DNA is very durable, being less susceptible to environmental degradation and physical and biological contamination than other components of blood evidence. DNA testing can also indicate when a crime scene sample is a mixture from several sources, and can often separate out different individuals' DNA from the mix. Of course, DNA can identify or exclude a suspect with much higher confidence than any other available test because it provides more precise information.²⁵

Chapter Three details the scientific underpinnings and technical procedures for obtaining a DNA fingerprint. DNA fingerprinting allows highly accurate identification of individuals by isolating and identifying certain sequences of DNA whose length and number vary greatly from person to person, and comparing the pattern of these DNA sequences found in crime samples with a suspect's pattern to determine if the DNA patterns match.²⁶ The authors explain the

24. *Id.* at 20-22.

25. *See id.* at 25-27.

26. In the procedure called RFLP (Restriction Fragment Length Polymorphism) analysis, these DNA fragments are separated by size using an electrical current which pulls smaller fragments farther through a porous gel than larger fragments. The resulting series of DNA bands are radioactively tagged and then made visible by exposure to a sheet of film. The resulting "picture" is a column of bands positioned according to size and superficially resembling the UPC bar code found on commercial goods. By comparing the band pattern of a crime scene sample with the patterns from the victim and any suspects, technicians will determine if any of the DNA in the sample matches that of a suspect. Once a match, or inclusion, is declared, the

basic genetic principles which allow DNA fingerprinting to work and thoroughly cover the various steps performed in obtaining a DNA fingerprint and declaring a match. The discussion includes an extensive description of what promises to be the foremost DNA analysis technique in the near future, PCR-based typing. PCR typing is based on a procedure, called polymerase chain reaction amplification, that increases the amount of available DNA by duplicating it over and over. PCR analysis presents several advantages over traditional (RFLP) analysis, being a faster and relatively simpler operation that can be performed on even minute amounts of DNA.²⁷

Once one of these testing methods yields a match between the suspect's DNA pattern and the pattern found in the crime scene sample, the suspect is said to be "included" in the class of possible perpetrators of the crime. An inclusion does not, however, automatically mean that the suspect committed the crime, since someone else with the same DNA pattern may have been the actual perpetrator. The likelihood that someone else with the same DNA pattern may have been the source of the crime scene sample is determined by statistical analysis of the occurrence of that particular DNA pattern in the general population. Thus if a DNA pattern appears with high frequency in the population, a match between a suspect and a crime scene sample will be less significant than if the pattern appears infrequently. Moreover, DNA fingerprints usually test for several different DNA sequences. Each DNA sequence has its own frequency of occurrence in the general population. The overall frequency for a DNA fingerprint that tests multiple sequences is calculated by multiplying the individual frequencies of each DNA sequence.²⁸ This frequency calculation method is called the product rule.

Statistical analysis methods such as the product rule are at the center of a maelstrom of controversy in the DNA wars. Critics argue that the product rule underestimates the frequency of the suspect's DNA pattern in the general population, thus overestimating the

statistical likelihood that the defendant is not the source (i.e., that the match occurred randomly) is evaluated using population databases which estimate the frequency of the tested DNA fragments in the population.

27. See MOENSSENS, *supra* note 12, at 910-12.

28. Thus, if a DNA fingerprint tests for sequence A and sequence B, and the individual frequency of sequence A in the general population is 1 in 100, or .01, and the frequency of sequence B is 1 in 1000, or .001, the frequency of a DNA fingerprint showing both A and B will be $.001 \times .01 = .00001$ or 1 in 100,000. Clearly, as more sequences are tested for, the frequency for the overall DNA pattern can quickly reach one in millions or even billions.

likelihood that the suspect is the source of the crime scene sample DNA. These critics argue that analysis of the frequency of DNA patterns in the general population, or even in specific ethnic populations, ignores the possibility of smaller subpopulations in which the frequency of the suspect's DNA pattern may occur with greater frequency than in the larger population.²⁹ Proponents of DNA evidence counter that no evidence shows that the existence of subpopulations significantly alters the frequency calculations.³⁰ Furthermore, proponents have proposed alternatives to the product rule that are conservative (pro-defendant) methods of statistical analysis that more than account for any unknown bias such as the subpopulation problem.³¹ Critics have responded by attacking these alternative methods as inaccurate calculations that violate population genetics principles.³² Some renowned scientists, attempting to quiet the storm of controversy, point out that although the alternative methods may not be the *best* statistical evaluation method, they are so conservative that no one could argue that their inaccuracy harms the defendant.³³

One weakness of the book is its relatively cursory treatment of this statistical analysis controversy. A satisfactory overview of this issue and the complex field of population genetics is an admittedly difficult task given the scope of the book. Nevertheless the importance of this element of DNA evidence and its starring role in the current DNA debates calls for more comprehensive coverage than the authors provide.

The authors next include a short chapter on DNA parentage testing. Although they have received far less press and have not figured significantly in the debates on DNA fingerprinting reliability, parentage testing cases are the most common application of the technology.³⁴ DNA parentage testing applications include child support enforcement, criminal paternity, identifying human remains and medical genetics.³⁵ Parentage DNA testing, like forensic DNA analysis, has considerable advantages over conventional blood analysis, but also shares with forensic DNA testing the same difficulties that can affect reliability, such as proper performance of

29. See MOENSSENS, *supra* note 12, at 924-25.

30. See *id.* at 925-26.

31. See *id.* at 926-27.

32. See *id.* at 927-28.

33. See, e.g., Eric S. Lander & Bruce Budowle, *DNA Fingerprinting Dispute Laid to Rest*, 371 NATURE 735 (1994).

34. COLEMAN & SWENSON, *supra* note 1, at 62.

35. *Id.* at 64.

testing procedures, chain of custody, degraded samples, laboratory quality control and statistical population analysis. Interestingly, opponents of forensic DNA testing have not been as vocal in attacking the reliability of DNA testing for parentage purposes.³⁶ This is true even though parentage tests often provide evidence in criminal cases, for example by identifying human remains or testing fetuses for proof of criminal activity such as rape or child molestation.³⁷ The lack of opposition is even more surprising considering that the proficiency of testing laboratories is less closely scrutinized and more susceptible to variations in quality in parentage testing than in the forensic setting.³⁸ This selectivity in criticism may, as the authors point out, provide insight into the true significance of many of the objections to forensic DNA testing.

The discussion then moves from the complexities of DNA technology in the laboratory to the complexities of DNA technology in the courtroom. In chapter Five the authors reach the crux of the DNA controversy: the difficulties of incorporating complex scientific evidence into our legal system. In their description of the relevant legal rules governing DNA admissibility, the authors conscientiously explain all legal provisions in lay terms. They succinctly describe the nature of evidence, including rules on opinion testimony and expert opinions, as well as basic principles of discovery.³⁹ The authors describe how discovery has sometimes been a source of contention, but focus on admissibility as the central legal issue in DNA fingerprinting.⁴⁰

The DNA controversy centers on the admissibility of DNA fingerprints at trial. Scientific evidence, such as DNA fingerprints, must meet a certain reliability threshold before it can be admitted.⁴¹ The rationale for this special evidentiary standard is that scientific evidence, by its very nature, is not susceptible to the adversarial system's traditional measures for ensuring reliability, such as cross-examination and opposing evidence. Factfinders, whether judge or jury, do not have the requisite technical knowledge to evaluate the reliability of the scientific evidence. In fact, this is the very reason such evidence is needed in the first place, to provide the factfinder with technical knowledge and information it does not itself possess.

36. The same conspicuous silence is evident when forensic DNA testing is used to exculpate the defendant.

37. See COLEMAN & SWENSON, *supra* note 1, at 66-67.

38. *Id.* at 70-71.

39. *Id.* at 75-77.

40. *Id.* at 77.

41. See *id.*

In addition, such evidence can often have an aura of infallibility that can so overwhelm factfinders, especially lay juries, that they may afford the evidence disproportionate weight.⁴²

Courts have applied various standards to measure the reliability of scientific evidence. The authors provide a concise account of these standards and their historical development. Courts today determine admissibility using either the *Frye* rule, which requires that scientific evidence must be "generally accepted" by the scientific community before being admitted,⁴³ or the Federal Rules of Evidence (FRE) which require that scientific evidence be relevant⁴⁴ and helpful.⁴⁵

Until 1993 it was unclear whether the FRE, which nowhere mention general acceptance, had superseded the *Frye* rule. Some federal circuits held that the FRE abolished *Frye*, while others read the FRE as incorporating the *Frye* rule into their reliability requirement.⁴⁶ The United States Supreme Court resolved the split in the recent landmark case *Daubert v. Merrell Dow Pharmaceuticals*, holding that *Frye* did not survive the enactment of the FRE that

42. DNA fingerprints clearly carry this aura since the match frequencies are so astronomical that they seem to prove indisputably the defendant's guilt.

43. COLEMAN & SWENSON, *supra* note 1, at 77. The *Frye* rule originated in a 1923 federal court of appeals decision that excluded the results of a primitive lie-detector test as too unreliable. *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). In a much-quoted statement, the court declared:

Just when a scientific principle or discovery crosses the line between experimental and demonstrable stages is difficult to define. Somewhere in the twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.

Frye, 293 F. at 1014.

44. FED. R. EVID. 402.

45. FED. R. EVID. 702 ("If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise."). Helpfulness incorporates reliability since unreliable evidence will not be helpful. See *Daubert v. Merrell Dow Pharmaceuticals*, *infra* note 47. The FRE are directly applicable only to federal courts, but many states have evidence codes patterned after, and identical in relevant part, to the FRE.

46. States with evidence codes patterned after the FRE were similarly struggling to reconcile the FRE and *Frye*. Like the federal courts, these states split on whether their evidence codes superseded *Frye*.

scientific evidence is to be evaluated using the FRE's relevance and helpfulness standard.⁴⁷

In addition to covering these various evidentiary rules, the authors note two additional legal standards affecting DNA admissibility, the emergence in some states of legislated admissibility and the role of expert witnesses. Several states have enacted statutes mandating the admissibility of DNA evidence without antecedent expert testimony on the technique's reliability.⁴⁸ This legislated admissibility applies only to the underlying theories and technology of DNA fingerprinting, not issues such as statistical evaluation methods or proper performance of testing protocols that currently are the primary points of contention.⁴⁹ Nor do the statutes apply to subsequently developed DNA analysis methods.⁵⁰ Nevertheless, legislated admissibility promises to be a growing trend in the field.⁵¹

Our legal system's reliance on partisan experts to bring scientific evidence to the courtroom also has a profound effect on DNA admissibility. Coleman and Swenson make note of the proliferation of "professional experts" who are not always well-qualified or impartial enough to be relied on to provide the court with such complex and often outcome-determinative material as DNA evidence. Some suggestions for curtailing this phenomenon include implementing rigorous academic, professional and ethical qualification requirements for expert witnesses and increased use of court-appointed experts to promote impartiality.⁵²

The authors next present a section, highly useful to practitioners, describing defense strategies and the main lines of attack on forensic DNA testing. The authors survey the primary points of contention, including experts' conflicts of interest, unreliable chain of custody,

47. 113 S. Ct. 2786, 2794 (1993). Like the FRE, *Daubert* does not automatically control state evidentiary law, but since many state codes are identical to the FRE in relevant part, such states may choose to follow the U.S. Supreme Court's interpretation of the FRE and *Frye*. Some of these states had already abandoned *Frye* for the federal approach pre-*Daubert*. See, e.g., *Prater v. State*, 820 S.W.2d 429 (Ark. 1991); *Santiago v. State*, 510 A.2d 488 (Del. 1986); *Rivera v. State*, 840 P.2d 933 (Wyo. 1992). Others have since adopted the *Daubert* reasoning and abolished *Frye*. See, e.g., *City of Fargo v. McLaughlin*, 512 N.W.2d 700 (N.D. 1994); *State v. Alberico*, 861 P.2d 192 (N.M. 1993). The remainder have yet to reject *Frye* in favor of *Daubert*.

48. COLEMAN & SWENSON, *supra* note 1, at 80. In their appendix, the authors list these states, which include Alabama, Connecticut, Indiana, Louisiana, Maryland, Minnesota, Nevada, Tennessee, Virginia, and West Virginia. See *id.* at 113-20.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.* at 81-82.

technical inaccuracies (such as improper procedures or contamination of samples) and unreliable statistical analysis methods.⁵³ Unfortunately, as in the technical chapters, the authors provide insufficient coverage of the now-dominant statistical analysis controversy.

The authors briefly survey the trial and appeals processes. They review several appellate-level decisions regarding DNA admissibility. The authors also survey several California appellate decisions, concluding that California courts unanimously accept the theory and methods of RFLP testing, but differ in their rulings on admissibility of statistical analysis results.⁵⁴

Finally, the authors discuss the role of DNA fingerprints in providing relief from erroneous convictions. The authors state that about a dozen men have had convictions reversed and been released from prison when DNA evidence excluded them as the perpetrators of the crime for which they had been convicted.⁵⁵ According to the authors, an additional thousand men annually are arrested as crime suspects and then released without being charged when DNA evidence exonerates them.⁵⁶ The authors note that also some of the most vociferous objectors to admitting *inculpatory* DNA evidence ardently advocate use of DNA evidence to *exculpate* the accused.⁵⁷ This dichotomy is certainly interesting. The point would be even more telling if the authors critically evaluated the justifications put forth by those who propose this dual standard, an evaluation the authors do not undertake.

With regard to inculpatory evidence, the authors note that, despite the contention surrounding DNA fingerprinting, the injustices predicted by opponents of the evidence have failed to materialize. For example, the record shows no re-test of DNA evidence resulting in inconsistent conclusions from the original analysis.⁵⁸

The final chapter of the book covers the early stages of the Simpson trial, as the prosecution and defense teams were gearing up for the battle over DNA evidence. While one might be tempted to dismiss this chapter as irrelevant now that the trial is over, the discussion is actually an absorbing case study of the contours of a DNA battle. The authors present an analysis of defense and prosecution strategies, as well as detailed commentary regarding the experts

53. *Id.* at 82-86.

54. *See id.* at 88-89.

55. *Id.* at 89.

56. *See id.* at 112.

57. *Id.* at 90.

58. *Id.* at 90.

lined up on either side. The description of the experts, their backgrounds, qualifications and personalities, enlivens the discussion and illuminates how these elements impact the experts' testimony and contribute to the contentious nature of the DNA controversy. This perspective is particularly relevant since the experts employed in the Simpson case are some of the main players in the DNA controversy and will continue to figure prominently as the debates continue.

CONCLUSION

The authors, in their afterword, conclude that "the prospects for ending the DNA War quickly are dim."⁵⁹ Although they believe that developments in the technology will eventually compel complete acceptance of DNA evidence, they oppose deferring the use of such a powerful tool until absolutely no scientific disagreements exist. They note that "[t]he DNA revolution has brought into sharp focus how hard it is for the judicial system to evaluate and incorporate new scientific technologies,"⁶⁰ and posit that the DNA controversy "speak[s] more to the nature of our legal system and the politics and economics of the scientific community than to the soundness of the technology."⁶¹

Knowledge and information are the key to a better understanding of these revolutionary technologies. Jurists can no longer afford the scientific illiteracy that so characterizes the legal field. *DNA in the Courtroom* counteracts this phenomenon of illiteracy by providing a concise, yet comprehensive, introduction to the complex scientific and legal issues of DNA fingerprinting. The work is worthwhile, entertaining and accessible reading for jurists, journalists and the general public alike.

59. *Id.* at 111.

60. *Id.* at 112.

61. *Id.*

INDEXES

The following indexes include references to all articles and comments published in Volumes 1-10. These indexes allow the reader to locate articles and comments by author's name, issue of publication, subject matter or title. Similar indexes, linked to abstracts for each article and comment, appear on the High Technology Law Journal's site on the World Wide Web at <http://server.berkeley.edu/HTLJ/>.

TABLE OF CONTENTS

AUTHOR INDEX.....	447
ISSUE INDEX.....	460
SUBJECT INDEX.....	466
TITLE INDEX	475

AUTHOR INDEX

A

Ausubel, Warren

- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Issue 4:1 (Spring 1989)

B

Barkan, David

- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, Issue 7:2 (Fall 1992)

Bayer, Barry

- *Computerized Citation Checking Revisited*, Issue 3:2 (Fall 1988)

Beard, Joseph

- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Issue 8:1 (Spring 1993)

Bell, Suzanne

- *Software Product Liability: Understanding and Minimizing the Risks*, Issue 5:1 (Spring 1990)

Berring, Robert

- *Full-Text Databases and Legal Research: Backing Into the Future*, Issue 1:1 (Spring 1986)

Brooks, Timothy

- *Regulating International Trade in Launch Services*, Issue 6:1 (Spring 1991)

Burgunder, Lee

- *An Emerging Theory of Computer Software Genericism*, Issue 2:2 (Fall 1987)

C**Cabot, Howard Ross**

- *Watercloud Muddies the Water for Patent Coverage Disputes*, Issue 8:2 (Fall 1993)

Carleton, Dennis M.

- *A Behavior-Based Model for Determining Software Copyright Infringement*, Issue 10:2 (Fall 1995)

Crisman, Thomas

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Cross, George

- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Issue 1:2 (Fall 1986)

Cunningham, Brian

- *Emerging Product Liability Issues in Biotechnology*, Issue 3:2 (Fall 1988)

D**Danilenko, Gennady**

- *Outer Space and the Multilateral Treaty-Making Process*, Issue 4:2 (Fall 1989)

Darr, Frank

- *Regulation of Alternative Operator Services*, Issue 6:1 (Spring 1991)

Debessonnet, Cary

- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Issue 1:2 (Fall 1986)

Denemark, Howard

- *The Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth,"* Issue 8:2 (Fall 1993)

Dorney, Maureen

- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Issue 5:2 (Fall 1990)

Douros, Timothy J.

- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Issue 10:2 (Fall 1995)

E**Eisenschmidt, Lori E.**

- *The Commercial Law of Internet Security*, Issue 10:2 (Fall 1995)

F**Feldman, Miles**

- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Issue 9:1 (Spring 1994)

Fought, Bonnie

- *Legal Aspects of the Commercialization of Space Transportation Systems*, Issue 3:1 (Spring 1988)

Fox, Eleanor

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Issue 6:1 (Spring 1991)

G**Gill, Christopher**

- *Medical Expert Systems: Grappling with Issues of Liability*, Issue 1:2 (Fall 1986)

Gruner, Richard

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Issue 1:2 (Fall 1986)

H**Hasan, Salim A.**

- *A Call for Reconsideration of the Strict Utility Standard in Chemical Patent Practice*, Issue 9:2 (Fall 1994)

Heckman, Carey

- *An Emerging Theory of Computer Software Genericism*, Issue 2:2 (Fall 1987)

Herman, Karen Goldman

- *Issues in the Regulation of Bioengineered Food*, Issue 7:1 (Spring 1992)

Hertz, Ellen

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Issue 5:2 (Fall 1990)

Hogle, Doreen

- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Issue 5:1 (Spring 1990)

Hurewitz, Barry J.

- *Non-Proliferation and Free Access to Outer Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Issue 9:2 (Fall 1994)

I J**Johnson, Dana**

- *The Impact of International Law and Treaty Obligations on United States Military Activities in Space*, Issue 3:1 (Spring 1988)

Johnston, Sean

- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Issue 4:2 (Fall 1989)

Johnston, Pamela

- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Issue 2:2 (Fall 1987)

Jones, Richard

- *Is There a Property Interest in Scientific Research Data?*, Issue 1:2 (Fall 1986)

Jorde, Thomas

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Issue 4:1 (Spring 1989)

K**Kasch, Steven**

- *The Semiconductor Chip Protection Act: Past, Present, and Future*, Issue 7:1 (Spring 1992)

Koffsky, Mark

- *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Issue 9:1 (Spring 1994)

Krauthaus, Patricia

- *Secured Financing and Information Property Rights*, Issue 2:2 (Fall 1987)

Kuo, John

- *Sales/Use Taxation of Software: An Issue of Tangibility*, Issue 2:1 (Spring 1987)

Kushan, Jeffrey

- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Issue 6:1 (Spring 1991)

L**Lacroix, Gerard**

- *Protecting the "Look and Feel" of Computer Software*, Issue 1:2 (Fall 1986)

Lagod, Martin

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Issue 5:2 (Fall 1990)

Larson, Alexander

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Issue 6:2 (Fall 1991)

Lee, Mavis

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Issue 6:2 (Fall 1991)

Lee, Michele

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Issue 6:2 (Fall 1991)

Lemley, Mark A.

- *Convergence in the Law of Software Copyright?*, Issue 10:1 (Spring 1995)

Levy, Lawrence

- *Software Product Liability: Understanding and Minimizing the Risks*, Issue 5:1 (Spring 1990)

Loewenheim, Ulrich

- *Legal Protection for Computer Programs in West Germany*, Issue 4:2 (Fall 1989)

Lunney, Glynn

- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Issue 5:1 (Spring 1990)

M**Maatz, Claire Turcotte**

- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Issue 7:1 (Spring 1992)

Manheim, William

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, Issue 2:1 (Spring 1987)

Martin, Patricia

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Issue 5:2 (Fall 1990)

May, Randolph

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Issue 8:1 (Spring 1993)

McGarity, Thomas

- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Issue 9:1 (Spring 1994)

McGraw, Molly

- *Sound Sampling Protection and Infringement in Today's Music Industry*, Issue 4:1 (Spring 1989)

McManis, Charles

- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Issue 8:1 (Spring 1993)

McNally, Janine

- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Issue 5:1 (Spring 1990)

Meeker, Heather J.

- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Issue 9:2 (Fall 1994)

Merges, Robert

- *Uncertainty and the Standard of Patentability*, Issue 7:1 (Spring 1992)
- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Issue 3:1 (Spring 1988)

Methvin, Gaynell

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Michel, Suzanne

- *The Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, Issue 7:2 (Fall 1992)

N**Naumann, Adrienne**

- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Issue 1:1 (Spring 1986)

Nicholson, Bradley J.

- *The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM*, Issue 10:1 (Spring 1995)

Nimmer, Raymond

- *Secured Financing and Information Property Rights*, Issue 2:2 (Fall 1987)

O P**Pace, Kimberly**

- *The Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, Issue 9:1 (Spring 1994)

Paepke, C. Owen

- *An Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, Issue 2:1 (Spring 1987)

Paredes, Troy

- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?* Issue 9:2 (Fall 1994)

Pinheiro, John

- *Protecting the "Look and Feel" of Computer Software*, Issue 1:2 (Fall 1986)

Poulter, Susan

- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Issue 7:2 (Fall 1992)

Q R**Reisman, Joseph**

- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Issue 10:2 (Fall 1995)

Reynolds, Glenn

- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Issue 3:1 (Spring 1988)

Rich, Allen

- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Issue 5:2 (Fall 1990)

Robinson, George

- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, Issue 3:1 (Spring 1988)

Rosenkranz, E. Joshua

- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, Issue 2:1 (Spring 1987)

Rosler, Debra B.

- *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, Issue 10:1 (Spring 1995)

Rowland, Bertram

- *Legal Implications of Letter Licenses for Biotechnology*, Issue 1:1 (Spring 1986)

Rustad, Michael

- *The Commercial Law of Internet Security*, Issue 10:2 (Fall 1995)

S**Samuelson, Pamela**

- *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Issue 6:2 (Fall 1991)

Schroepfer, Terrence

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Issue 6:2 (Fall 1991)

Seecof, Benjamin

- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Issue 5:2 (Fall 1990)

Selbak, John

- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, Issue 9:2 (Fall 1994)

Silverman, Alexander

- *Intellectual Property Law and the Venture Capitalist Process*, Issue 5:1 (Spring 1990)

Steele, Lisa

- *The View From on High: Satellite Remote Sensing Technology and the Fourth Amendment*, Issue 6:2 (Fall 1991)

Stockdale, Donald

- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost*, Issue 7:2 (Fall 1992)

Stork, Anita

- *The Use of Arbitration in Copyright Disputes: IBM v. Fujitsu*, Issue 3:2 (Fall 1988)

Stovsky, Michael

- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Issue 6:2 (Fall 1991)

Sullivan, Lawrence A.

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Issue 5:2 (Fall 1990)

Sullivan, Barry

- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Issue 3:2 (Fall 1988)

T**Teece, David**

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Issue 4:1 (Spring 1989)

Thomas, John R.

- *The Question Concerning Patent Law and Pioneer Inventions*, Issue 10:1 (Spring 1995)

Traynor, Michael

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Issue 6:1 (Spring 1991)
- *Emerging Product Liability Issues in Biotechnology*, Issue 3:2 (Fall 1988)

U V W X Y Z**Weitz, David**

- *The Biological Deposit Requirement: A Means of Assuring Adequate Disclosure*, Issue 8:2 (Fall 1993)

Welch, Mark

- *Computerized Citation Checking Revisited*, Issue 3:2 (Fall 1988)

Whitt, Richard

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Issue 8:1 (Spring 1993)

Winters, Steven

- *The New Privacy Interest: Electronic Mail in the Workplace*, Issue 8:1 (Spring 1993)

Wrenn, Gregory

- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Issue 4:2 (Fall 1989)

Wright, Christopher

- *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, Issue 1:1 (Spring 1986)

Yin, Tung

- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Issue 8:2 (Fall 1993)

Zschau, Ed

- *Export Controls and America's Competitive Challenge*, Issue 1:1 (Spring 1986)

ISSUE INDEX

Issue 10:2

- *The Commercial Law of Internet Security*, Michael Rustad and Lori E. Eisenschmidt
- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Timothy J. Douros
- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Joseph M. Reisman
- *A Behavior-Based Model for Determining Software Copyright Infringement*, Dennis M. Carleton

Issue 10:1

- *Convergence in the Law of Software Copyright?*, Mark A. Lemley
- *The Question Concerning Patent Law and Pioneer Inventions*, John R. Thomas
- *The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, Debra B. Rosler
- *The Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM*, Bradley J. Nicholson

Issue 9:2

- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Heather J. Meeker
- *Non-Proliferation and Free Access to Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Barry J. Hurewitz
- *A Call for Reconsideration of the Strict Utility Standard in Chemical Patent Practice*, Salim A. Hasan
- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?*, Troy Paredes
- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, John Selbak

Issue 9:1

- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Thomas McGarity

- *The Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, Kimberly Pace
- *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Mark Koffsky
- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Miles Feldman

Issue 8:2

- *The Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth,"* Howard Denmark
- *Watercloud Muddies the Water for Patent Coverage Disputes*, Howard Ross Cabot
- *The Biological Deposit Requirement: A Means of Assuring Adequate Disclosure*, David Weitz
- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Tung Yin

Issue 8:1

- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Randolph May and Richard Whitt
- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Charles McManis
- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Joseph Beard
- *The New Privacy Interest: Electronic Mail in the Workplace*, Steven Winters

Issue 7:2

- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Susan Poulter
- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost?*, Donald Stockdale
- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, David Barkan

- *The Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, Suzanne Michel

Issue 7:1

- *Uncertainty and the Standard of Patentability*, Robert Merges
- *The Semiconductor Chip Protection Act: Past, Present, and Future*, Steven Kasch
- *Issues in the Regulation of Bioengineered Food*, Karen Goldman Herman
- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Claire Turcotte Maatz

Issue 6:2

- *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Pamela Samuelson
- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Alexander Larson and Terrence Schroepfer
- *The View From on High: Satellite Remote Sensing Technology and the Fourth Amendment*, Lisa Steele
- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Mavis Lee and Michele Lee
- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Michael Stovsky

Issue 6:1

- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Eleanor Fox and Michael Traynor
- *Regulation of Alternative Operator Services*, Frank Darr
- *Regulating International Trade in Launch Services*, Timothy Brooks
- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Jeffrey Kushan

Issue 5:2

- *The AT&T Antitrust Consent Decree: Should Congress Change the Rules?*, Lawrence A. Sullivan and Ellen Hertz

- *The Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research*, Patricia Martin
- *The Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More*, Allen Rich, Gaynell Methvin and Thomas Crisman
- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Maureen Dorney
- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Benjamin Seecof

Issue 5:1

- *Software Product Liability: Understanding and Minimizing the Risks*, Lawrence Levy and Suzanne Bell
- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Glynn Lunney
- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Doreen Hogle
- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Janine McNally
- *Intellectual Property Law and the Venture Capitalist Process*, Alexander Silverman

Issue 4:2

- *Legal Protection for Computer Programs in West Germany*, Ulrich Loewenheim
- *Outer Space and the Multilateral Treaty-Making Process*, Gennady Danilenko
- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Sean Johnston
- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Gregory Wrenn

Issue 4:1

- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Thomas Jorde and David Teece
- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Warren Ausubel

- *Sound Sampling Protection and Infringement in Today's Music Industry*, Molly McGraw

Issue 3:2

- *Emerging Product Liability Issues in Biotechnology*, Michael Traynor and Brian Cunningham
- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Barry Sullivan
- *The Use of Arbitration in Copyright Disputes: IBM v. Fujitsu*, Anita Stork
- *Computerized Citation Checking Revisited*, Mark Welch and Barry Bayer

Issue 3:1

- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Robert Merges and Glenn Reynolds
- *The Impact of International Law and Treaty Obligations on United States Military Activities in Space*, Dana Johnson
- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, George Robinson
- *Legal Aspects of the Commercialization of Space Transportation Systems*, Bonnie Fought

Issue 2:2

- *Secured Financing and Information Property Rights*, Raymond Nimmer and Patricia Krauthaus
- *An Emerging Theory of Computer Software Genericism*, Lee Burgunder and Carey Heckman
- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Pamela Johnston

Issue 2:1

- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, E. Joshua Rosenkranz
- *An Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, C. Owen Paepke

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, William Manheim
- *Sales/Use Taxation of Software: An Issue of Tangibility*, John Kuo

Issue 1:2

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Richard Gruner
- *An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information*, Cary Debessonet and George Cross
- *Protecting the "Look and Feel" of Computer Software*, John Pinheiro and Gérard Lacroix
- *Is There a Property Interest in Scientific Research Data?*, Richard Jones
- *Medical Expert Systems: Grappling with Issues of Liability*, Christopher Gill

Issue 1:1

- *Export Controls and America's Competitive Challenge*, Ed Zschau
- *Full-Text Databases and Legal Research: Backing Into the Future*, Robert Berring
- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Adrienne Naumann
- *Legal Implications of Letter Licenses for Biotechnology*, Bertram Rowland
- *The National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures*, Christopher Wright

SUBJECT INDEX

The references to each article in the list below include the authors' last names and the issue number. For example, Martin/Lagod 5:2 indicates an article written by Martin and Lagod that appeared in HTLJ issue 5:2.

A

- **abortion:** Martin/Lagod 5:2, Meeker 9:2
- **abstraction-filtration comparison test:** Lemley 10:1
- **active review:** Poulter 7:2
- **alternative operator services:** Darr 6:1
- **antitrust law:** Jorde/Teece 4:1, Lee/Lee 6:2, Lunney 5:1, Paredes 9:2, Stockdale 7:2, Sullivan/Hertz 5:2, Wright 1:1
- **arbitration:** Rich 5:2, Stork 3:2
- **artificial intelligence:** Debessonet/Cross 1:2, Gruner 1:2
- **AT&T consent decree:** Sullivan/Hertz 5:2
- **Atari:** Lunney 5:1

B

- **Baby Bells:** Sullivan/Hertz 5:2
- **bioengineered food:** Herman 7:1
- **biological deposit requirement:** Weitz 8:2
- **biological material transfers:** Rowland 1:1
- **biomedical ethics:** Meeker 9:2, Reisman 10:2, Rosenkranz 2:1
- **biotechnology (see also genetic engineering)**
 - **generally:** Ausubel 4:1, Hasan 9:2, Herman 7:1, Johnston 4:2, Maatz 7:1, Naumann 1:1, Rowland 1:1, Traynor/Cunningham 3:2, Weitz 8:2
 - **food:** Herman 7:1
 - **physician-researcher:** Maatz 7:1
 - **product liability:** Fox/Traynor 6:1, Stovsky 6:2
 - **regulation:** Herman 7:1

C

- **CPUC:** Manheim 2:1
- **California Public Utilities Commission:** Manheim 2:1
- **causation:** Poulter 7:2
- **cell-line:** Dorney 5:2
- **chemical industry:** Hasan 9:2
- **Clipper scheme:** Koffsky 9:1
- **closed system:** Lunney 5:1
- **colorization:** McNally 5:1
- **Comment "k":** Fox/Traynor 6:1

- **computer animation:** Beard 8:1, Selbak 9:2, Sullivan 3:2
- **computer-generated re-enactments:** Sullivan 3:2
- **computer hardware**
 - **chip piracy:** Kasch 7:1
 - **copyright (see also copyright):** Nicholson 10:1
 - **reverse engineering:** Kasch 7:1
 - **Semiconductor Chip Protection Act of 1984:** Kasch 7:1
- **computer research:** Berring 1:1
- **computer security:** Rustad/Eisenschmidt 10:2
- **computer software**
 - **generally:** Burgunder/Heckman 2:2, Feldman 9:1, Kuo 2:1, Lunney 5:1, Pinheiro/Lacroix 1:2, Samuelson 6:2
 - **behavior:** Carleton 10:2
 - **copyright (see also copyright):** Barkan 7:2, Burgunder/Heckman 2:2, Carleton 10:2, Lemley 10:1, Loewenheim 4:2, McManis 8:1, Nicholson 10:1, Pinheiro/Lacroix 1:2, Rosler 10:1, Samuelson 6:2, Stork 3:2, Wrenn 4:2
 - **European Community Directive:** McManis 8:1
 - **networks:** Rustad/Eisenschmidt 10:2
 - **Object-Oriented Programming:** Barkan 7:2
 - **patent:** Barkan 7:2
 - **product liability (see also product liability):** Gill 1:2, Levy/Bell 5:1
 - **reverse engineering:** McManis 8:1
 - **user interfaces:** Samuelson 6:2
 - **vendors:** Levy/Bell 5:1
- **computer systems:** Debessonet/Cross 1:2, Gruner 1:2
- **conceptual retrieval:** Debessonet/Cross 1:2
- **confidentiality:** Feldman 9:1
- **conflict of interest**
 - **physician-researcher:** Maatz 7:1
 - **informed consent:** Maatz 7:1
- **constitutional law (see also First Amendment, Fourth Amendment):** Robinson 3:1
- **contract law:** Rowland 1:1
- **contract liability:** Levy/Bell 5:1
- **Cooperative Research Act of 1984:** Wright 1:1
- **copyright**
 - **generally:** Jones 1:2, Loewenheim 4:2, Paepke 2:1, Stork 3:2, Wrenn 4:2
 - **abstraction-filtration comparison test:** Lemley 10:1
 - **Act of 1976, Section 102(b) of:** Samuelson 6:2
 - **biotechnology:** Hogle 5:1
 - **computer animation:** Beard 8:1
 - **computer hardware:** Nicholson 10:1
 - **computer software (see also computer software):** Barkan 7:2, Burgunder/Heckman 2:2, Carleton 10:2, Loewenheim

- 4:2, McManis 8:1, Nicholson 10:1, Rosler 10:1, Pinheiro/Lacroix 1:2, Samuelson 6:2, Stork 3:2, Wrenn 4:2
- **fair use:** McManis 8:1, Seecof 5:2
- **misuse:** McManis 8:1, Paredes 9:2
- **Object-Oriented Programming:** Barkan 7:2
- **corporate venue:** Rich 5:2
- **credit law:** Nimmer/Krauthaus 2:2

D

- **database:** Rosler 10:1
- **digital manipulation:** Beard 8:1, Seecof 5:2
- **disclosure requirement:** Weitz 8:2
- **doctrine of equivalents:** Douros 10:2, Kushan 6:1, Thomas 10:1
- **duty to defend:** Cabot 8:2
- **duty to rescue:** Rosenkranz 2:1

E

- **EPA:** McGarity 9:1
- **e-mail (see electronic mail)**
- **economics of patent law:** Merges 7:1
- **electricity:** Manheim 2:1
- **electronic mail**
 - **business:** Winters 8:1
 - **employee rights:** Winters 8:1
 - **privacy rights:** Winters 8:1
- **electronic surveillance:** Koffsky 9:1
- **employment**
 - **electronic mail:** Winters 8:1
 - **law generally:** Feldman 9:1
 - **privacy rights:** Winters 8:1
- **energy:** Manheim 2:1
- **enhanced service providers:** May/Whitt 8:1
- **encryption:** Koffsky 9:1
- **environmental law:** Ausubel 4:1, Robinson 3:1
- **Environmental Protection Agency (EPA):** McGarity 9:1
- **equal protection:** Yin 8:2
- **equitable patent protection:** Kushan 6:1
- **equivalents, doctrine of:** Douros 10:2 ; Kushan 6:1; Thomas 10:1
- **ethics**
 - **biomedical:** Meeker 9:2, Reisman 10:2, Rosenkranz 2:1
 - **engineering:** Pace 9:1
 - **legal:** Pace 9:1
- **European Community Directive on Software Reverse Engineering:** McManis 8:1, Rosler 10:1
- **evidence:** Johnston 2:2, Selbak 9:2, Sullivan 3:2
- **excised tissue:** Dorney 5:2, Meeker 9:2

- expert systems
 - legal: Gruner 1:2
 - medical: Gill 1:2
- expert testimony: Johnston 2:2, Poulter 7:2, Selbak 9:2
- experimental use exception: Michel 7:2
- exports: Zschau 1:1

F

- FCC: Darr 6:1, May/Whitt 8:1
- FDA: Ausubel 4:1
- FERC: Manheim 2:1
- fact finding
 - legal: Denmark 8:2
 - scientific: Denmark 8:2
- fair use
 - generally: Seecof 5:2
 - computer animation: Beard 8:1
 - computer software: McManis 8:1
 - reverse engineering: McManis 8:1
- Federal Communications Commission (FCC): Darr 6:1, May/Whitt 8:1
- Federal Department of Agriculture (FDA): Ausubel 4:1
- Federal Energy Regulatory Commission (FERC): Manheim 2:1
- federal funding: McGarity 9:1
- federal grants: McGarity 9:1
- Federal Rules of Evidence: Selbak 9:2
- film: Beard 8:1, McNally 5:1
- finance law: Nimmer/Krauthaus 2:2
- First Amendment: Merges/Reynolds 3:1, Yin 8:2
- food, bioengineered: Herman 7:1
- Food and Drug Administration (FDA): Ausubel 4:1
- Fourth Amendment: Koffsky 9:1, Steele 6:2
- free-rider problem: Paepke 2:1
- free trade: Brooks 6:1
- freedom of the press: Yin 8:2

G

- General Agreement on Tariffs and Trade (GATT): Brooks 6:1
- genetic engineering (see also biotechnology)
 - generally: Ausubel 4:1, Johnston 4:2, Naumann 1:1, Rosenkranz 2:1, Traynor/Cunningham 3:2
 - food: Herman 7:1

H

- Hand formula: Douros 10:2

- hardware (see computer hardware)
- high technology innovation (see also industrial policy): Jorde/Teece 4:1, Thomas 10:1
- human tissue: Dorney 5:2, Meeker 9:2

I

- IVF: Martin/Lagod 5:2, Meeker 9:2
- image processing: Seecof 5:2
- in vitro fertilization (IVF): Martin/Lagod 5:2, Meeker 9:2
- inducement: Cabot 8:2
- industrial policy: Jorde/Teece 4:1, May/Whitt 8:1
- information services: May/Whitt 8:1
- information technology: Nimmer/Krauthaus 2:2
- informed consent: Dorney 5:2, Maatz 7:1
- insurance: Cabot 8:2
- intellectual property: Burgunder/Heckman 2:2, Kuo 2:1, Nimmer/Krauthaus 2:2, Rowland 1:1, Samuelson 6:2
- international trade: Zschau 1:1
- Internet: Rustad/Eisenschmidt 10:2

J

- joint ventures: Stockdale 7:2, Wright 1:1
- Judicial Improvements and Access to Justice Act: Rich 5:2
- junk science: Poulter 7:2

KL

- legal expert systems: Gruner 1:2
- legal research: Berring 1:1
- licensing: Lunney 5:1, Rustad/Eisenschmidt 10:2
- litigation: Wrenn 4:2
- lock-out chip: Lunney 5:1
- look and feel: Burgunder/Heckman 2:2, Carleton 10:2; Pinheiro/Lacroix 1:2, Samuelson 6:2;

M

- medical expert systems: Gill 1:2
- military space technology (see also space law): Johnson 3:1
- missile technology control regime: Hurewitz 9:2
- misuse: McManis 8:1, Paredes 9:2
- misappropriation: Paepke 2:1
- monopoly: Lunney 5:1
- motions to remand: Rich 5:2

N

- **NCRA:** Lee/Lee 6:2
- **NEA:** McGarity 9:1
- **NFPA:** McNally 5:1
- **NIH:** McGarity 9:1
- **NSF:** McGarity 9:1
- **National Cooperative Research Act (NCRA):** Lee/Lee 6:2
- **National Endowment for the Arts (NEA):** McGarity 9:1
- **National Film Preservation Act (NFPA):** McNally 5:1
- **National Institutes of Health (NIH):** McGarity 9:1
- **National Science Foundation (NSF):** McGarity 9:1
- **national security:** Zschau 1:1
- **negligence:** Fox/Traynor 6:1, Stovsky 6:2
- **Nintendo:** Lunney 5:1

O

- **object-oriented programming:** Barkan 7:2
- **obviousness:** Merges 7:1
- **on-line services:** Yin 8:2
- **open fields doctrine:** Steele 6:2
- **Outer Space Treaty:** Hurewitz 9:2

P

- **PCS:** Larson/Schroepfer 6:2
- **PURPA:** Manheim 2:1
- **parent/child relationship**
- **Particularity Clause:** Koffsky 9:1
- **patent law**
 - **generally:** Cabot 8:2, Hasan 9:2, Johnston 4:2, Loewenheim 4:2, Paepke 2:1, Weitz 8:2, Wrenn 4:2
 - **biological deposit requirement:** Weitz 8:2
 - **computer software:** Barkan 7:2
 - **disclosure requirement:** Weitz 8:2
 - **doctrine of equivalents:** Douros 10:2, Kushan 6:1, Thomas 10:1
 - **economic analysis:** Merges 7:1
 - **equitable patent protection:** Kushan 6:1
 - **experimental use exception:** Michel 7:2
 - **Hand formula applied to:** Douros 10:2
 - **medical techniques:** Reisman 10:2
 - **object-oriented programming:** Barkan 7:2
 - **obviousness:** Merges 7:1
 - **patent infringement:** Cabot 8:2
 - **inducement:** Cabot 8:2
 - **protein:** Kushan 6:1
 - **surgical techniques:** Reisman 10:2

- uncertainty: Merges 7:1
- utility requirement: Hasan 9:2
- peer review: McGarity 9:1
- **Personal Communication Services (PCS):** Larson/Schroepfer 6:2
- **physician-researcher:** Maatz 7:1
- **power:** Manheim 2:1
- **preembryo:** Martin/Lagod 5:2
- **preembryonic research:** Martin/Lagod 5:2
- **preemption:** McManis 8:1
- **privacy:** Winters 8:1
- **product liability:** Fox/Traynor 6:1, Gill 1:2, Levy/Bell 5:1, Stovsky 6:2, Traynor/Cunningham 3:2
- **production joint ventures:** Stockdale 7:2
- **property rights**
 - generally: Jones 1:2, Rowland 1:1
 - in human body: Dorney 5:2
- **proprietary information:** Feldman 9:1
- **protein patents and technology:** Kushan 6:1
- **public utilities:** Manheim 2:1
- **Public Utilities Regulatory Policy Act of 1978 (PURPA):** Manheim 2:1

QR

- **radio spectrum allocation:** Larson/Schroepfer 6:2
- **Regional Bell Operating Companies (RBOCs):** Sullivan/Hertz 5:2
- **reanimation:** Beard 8:1
- **regulation**
 - generally: Sullivan/Hertz 5:2
 - **bioengineered food:** Herman 7:1
 - **genetic engineering:** Naumann 1:1
 - **telephone:** Darr 6:1, May/Whitt 8:1
- **removal procedures:** Rich 5:2
- **reproductive rights:** Martin/Lagod 5:2
- **reproductive technologies:** Martin/Lagod 5:2, Meeker 9:2
- **research / research and development**
 - **antitrust law:** Stockdale 7:2
 - **computer:** Berring 1:1
 - **conflict of interest:** Maatz 7:1
 - **cooperation (see also research - joint ventures):** Lee/Lee 6:2
 - **effect of patentability on:** Merges 7:1
 - **experimental use exception:** Michel 7:2
 - **federally funded:** Michel 7:2
 - **industry funded:** Maatz 7:1
 - **joint ventures (see also research - cooperation):** Stockdale 7:2

- legal: Berring 1:1
- **reverse engineering**
 - chips: Kasch 7:1
 - computer software: McManis 8:1
 - fair use: McManis 8:1
 - misuse: McManis 8:1

S

- **satellite**
 - imagery: Steele 6:2
 - launching services: Brooks 6:1
 - media and technology: Merges/Reynolds 3:1
 - remote sensing technology: Steele 6:2
- scanning: Seecof 5:2
- scientific evidence: Poulter 7:2, Selbak 9:2
- scientific research data: Jones 1:2
- search and seizure: Koffsky 9:1
- **Semiconductor Chip Protection Act of 1984**: Kasch 7:1
- software (see computer software)
- space law and policy: Brooks 6:1, Danilenko 4:2, Fought 3:1, Hurewitz 9:2, Johnson 3:1, Merges/Reynolds 3:1, Robinson 3:1
- state of the art defense (see also **product liability**): Stovsky 6:2
- statutory interpretation: Debessonnet/Cross 1:2
- still image processing: Seecof 5:2
- strict liability (see also **product liability**): Fox/Traynor 6:1, Stovsky 6:2

T

- tangible/intangible property: Kuo 2:1
- taxation: Kuo 2:1
- technology consortia: Lee/Lee 6:2
- telecommunications (see also telephone)
 - generally: Darr 6:1, Sullivan/Hertz 5:2
 - regulation of: Larson/Schroepfer 6:2
- telephone (see also telecommunications)
 - alternative operator services: Darr 6:1
 - enhanced service providers: May/Whitt 8:1
 - Federal Communications Commission: Darr 6:1, May/Whitt 8:1
 - industrial policy: May/Whitt 8:1
 - information services: May/Whitt 8:1
 - rate structures: May/Whitt 8:1
- tort liability: Fox/Traynor 6:1, Levy/Bell 5:1, Paepke 2:1, Poulter 7:2
- toxic torts: Poulter 7:2
- trade secret law: Feldman 9:1, Nicholson 10:1, Paepke 2:1

- **trademark law:** Loewenheim 4:2, Wrenn 4:2
- **tying:** Paredes 9:2

U

- **UAGA:** Dorney 5:2
- **unavoidably unsafe products defense (see also product liability):** Stovsky 6:2
- **uncertainty standard of patentability:** Merges 7:1
- **unfair competition:** Cabot 8:2, Loewenheim 4:2
- **Uniform Anatomical Gift Act (UAGA):** Dorney 5:2
- **Uniform Commercial Code (UCC):** Rustad/Eisenschmidt 10:2
- **university research**
 - **conflict of interest:** Maatz 7:1
 - **experimental use exception:** Michel 7:2
 - **informed consent:** Maatz 7:1
- **user interfaces, computer software:** Samuelson 6:2

V

- **venue:** Rich 5:2
- **video game:** Lunney 5:1

WXYZ

- **wireless communication:** Larson/Schroepfer 6:2
- **wiretap:** Koffsky 9:1
- **x-ray crystallography:** Hogle 5:1

TITLE INDEX

A

- *AT&T Antitrust Consent Decree: Should Congress Change the Rules?, The*, Lawrence A. Sullivan and Ellen Hertz, Issue 5:2 (Fall 1990)
- *Antitrust and International Competitiveness: Is Encouraging Production Joint Ventures Worth the Cost?*, Donald Stockdale, Issue 7:2 (Fall 1992)
- *Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information, An*, Cary Debessonnet and George Cross, Issue 1:2 (Fall 1986)
- *Atari Games v. Nintendo: Does a Closed System Violate the Antitrust Laws?*, Glynn Lunney, Issue 5:1 (Spring 1990)

B

- *Behavior-Based Model for Determining Software Copyright Infringement*, A, Dennis M. Carleton, Issue 10:2 (Fall 1995)
- *Biological Deposit Requirement: A Means of Assuring Adequate Disclosure, The*, David Weitz, Issue 8:2 (Fall 1993)
- *Biotechnology for Human Life and Health—The Special Case for a Negligence-Only Rule to Promote Critical Innovation*, Eleanor Fox and Michael Traynor, Issue 6:1 (Spring 1991)

C

- *Casting Call at Forest Lawn: The Digital Resurrection of Deceased Entertainers—A 21st Century Challenge for Intellectual Property Law*, Joseph Beard, Issue 8:1 (Spring 1993)
 - *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, Mark Koffsky, Issue 9:1 (Spring 1994)
 - *Commercial Law of Internet Security, The*, Michael Rustad and Lori E. Eisenschmidt, Issue 10:2 (Fall 1995)
 - *Computer Programs, User Interfaces, and Section 102(b) of the Copyright Act of 1976: A Critique of Lotus v. Paperback*, Pamela Samuelson, Issue 6:2 (Fall 1991)
-

- *Computer-Generated Re-Enactments as Evidence in Accident Cases*, Barry Sullivan, Issue 3:2 (Fall 1988)
- *Computerized Citation Checking Revisited*, Mark Welch and Barry Bayer, Issue 3:2 (Fall 1988)
- *Congressional Limits on Technological Alterations to Film: The Public Interest and the Artists' Moral Right*, Janine McNally, Issue 5:1 (Spring 1990)
- *Convergence in the Law of Software Copyright?*, Mark A. Lemley, Issue 10:1 (Spring 1995)
- *Copyright Misuse and Tying: Will Courts Stop Misusing Misuse?*, Troy Paredes, Issue 9:2 (Fall 1994)
- *Copyright for Innovative Biotechnological Research: An Attractive Alternative to Patent or Trade Secret Protection*, Doreen Hogle, Issue 5:1 (Spring 1990)
- *Court-Appointed Scientific Expert Witnesses: Unfettering Expertise*, Pamela Johnston, Issue 2:2 (Fall 1987)
- *Custom Kids and the Moral Duty to Genetically Engineer Our Children*, E. Joshua Rosenkranz, Issue 2:1 (Spring 1987)

D

- *Digital Litigation: The Prejudicial Effects of High Technology Animation in the Courtroom*, John Selbak, Issue 9:2 (Fall 1994)

E

- *Economic Interpretation of the Misappropriation Doctrine: Common Law Protection for Investments in Innovation*, An, C. Owen Paepke, Issue 2:1 (Spring 1987)
- *Emerging Product Liability Issues in Biotechnology*, Michael Traynor and Brian Cunningham, Issue 3:2 (Fall 1988)
- *Emerging Theory of Computer Software Genericism*, An, Lee Burgunder and Carey Heckman, Issue 2:2 (Fall 1987)
- *European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information*, The, Debra B. Rosler, Issue 10:1 (Spring 1995)
- *Experimental Use Exception to Infringement Applied to Federally Funded Inventions*, The, Suzanne Michel, Issue 7:2 (Fall 1992)
- *Export Controls and America's Competitive Challenge*, Ed Zschau, Issue 1:1 (Spring 1986)

F

- *Federal Intellectual Property Protection for Computer Software Audiovisual Look and Feel: The Lanham, Copyright, and Patent Acts*, Gregory Wrenn, Issue 4:2 (Fall 1989)
- *Federal Regulation of Genetically Engineered Food Additives and Pesticides*, Warren Ausubel, Issue 4:1 (Spring 1989)
- *Federal Regulation of Recombinant DNA Technology: Time for Change*, Adrienne Naumann, Issue 1:1 (Spring 1986)
- *Full-Text Databases and Legal Research: Backing Into the Future*, Robert Berring, Issue 1:1 (Spring 1986)

G

- *Ghost in the Machine: MAI Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM, The*, Bradley J. Nicholson, Issue 10:1 (Spring 1995)

H

- *High Technology Consortia: A Panacea for America's Competitiveness Problems?*, Mavis Lee and Michele Lee, Issue 6:2 (Fall 1991)
- *Human Preembryo, the Progenitors and the State: Toward a Dynamic Theory of Status, Rights, and Research, The*, Patricia Martin and Martin Lagod, Issue 5:2 (Fall 1990)

I

- *Impact of International Law and Treaty Obligations on United States Military Activities in Space, The*, Dana Johnson, Issue 3:1 (Spring 1988)
- *Information Services in the 1990s: A Case Study in Rethinking the Beneficial Uses of Industrial Policy*, Randolph May and Richard Whitt, Issue 8:1 (Spring 1993)
- *Innovation, Cooperation, and Antitrust: Striking the Right Balance*, Thomas Jorde and David Teece, Issue 4:1 (Spring 1989)
- *Intellectual Property Law and the Venture Capitalist Process*, Alexander Silverman, Issue 5:1 (Spring 1990)
- *Intellectual Property Production and Reverse Engineering of Computer Programs in the United States and the European Community*, Charles McManis, Issue 8:1 (Spring 1993)

- *Is There a Property Interest in Scientific Research Data?*, Richard Jones, Issue 1:2 (Fall 1986)
- *Issues in the Regulation of Bioengineered Food*, Karen Goldman Herman, Issue 7:1 (Spring 1992)
- *Issues of Property, Ethics and Consent in the Transplantation of Fetal Reproductive Tissue*, Heather J. Meeker, Issue 9:2 (Fall 1994)

J

- *Judicial Improvements and Access to Justice Act: New Patent Venue, Mandatory Arbitration and More, The*, Allen Rich, Gaynell Methvin and Thomas Crisman, Issue 5:2 (Fall 1990)

KL

- *Legal Aspects of the Commercialization of Space Transportation Systems*, Bonnie Fought, Issue 3:1 (Spring 1988)
- *Legal Implications of Letter Licenses for Biotechnology*, Bertram Rowland, Issue 1:1 (Spring 1986)
- *Legal Profession as a Standard for Improving Engineering Ethics: Should Engineers Behave like Lawyers?*, The, Kimberly Pace, Issue 9:1 (Spring 1994)
- *Legal Protection for Computer Programs in West Germany*, Ulrich Loewenheim, Issue 4:2 (Fall 1989)
- *Lending the Federal Circuit a Hand: An Economic Interpretation of the Doctrine of Equivalents*, Timothy J. Douros, Issue 10:2 (Fall 1995)

M

- *Medical Expert Systems: Grappling with Issues of Liability*, Christopher Gill, Issue 1:2 (Fall 1986)
- *Moore v. The Regents of the University of California: Balancing the Need for Biotechnology Innovation Against the Right of Informed Consent*, Maureen Dorney, Issue 5:2 (Fall 1990)

N

- *National Cooperative Research Act of 1984: A New Antitrust Regime for Joint Research and Development Ventures, The*, Christopher Wright, Issue 1:1 (Spring 1986)
- *New Privacy Interest: Electronic Mail in the Workplace, The*, Steven Winters, Issue 8:1 (Spring 1993)

- *New Telecommunications Technologies and Regulation: The Case of Personal Communications Services*, Alexander Larson and Terrence Schroepfer, Issue 6:2 (Fall 1991)
- *News Media Satellites and the First Amendment: A Case Study in the Treatment of New Technologies*, Robert Merges and Glenn Reynolds, Issue 3:1 (Spring 1988)
- *Non-Proliferation and Free Access to Outer Space: The Dual-Use Dilemma of the Outer Space Treaty and the Missile Technology Control Regime*, Barry J. Hurewitz, Issue 9:2 (Fall 1994)

O

- *Outer Space and the Multilateral Treaty-Making Process*, Gennady Danilenko, Issue 4:2 (Fall 1989)

P

- *Patent Protection for the Protein Products of Recombinant DNA Technology*, Sean Johnston, Issue 4:2 (Fall 1989)
- *Peer Review in Awarding Federal Grants in the Arts and Sciences*, Thomas McGarity, Issue 9:1 (Spring 1994)
- *Physicians and Surgeons as Inventors: Reconciling Medical Process Patents and Medical Ethics*, Joseph M. Reisman, Issue 10:2 (Fall 1995)
- *Post-Modern Printing Presses: Extending Freedom of the Press to Protect Electronic Information Services*, Tung Yin, Issue 8:2 (Fall 1993)
- *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, Michael Stovsky, Issue 6:2 (Fall 1991)
- *Protecting the "Look and Feel" of Computer Software*, John Pinheiro and Gerard Lacroix, Issue 1:2 (Fall 1986)
- *Protein Patents and the Doctrine of Equivalents: Limits on the Expansion of Patent Rights*, Jeffrey Kushan, Issue 6:1 (Spring 1991)

Q

- *Question Concerning Patent Law and Pioneer Inventions, The*, John R. Thomas, Issue 10:1 (Spring 1995)

R

- *Re-Examining Our Constitutional Heritage: A Declaration of First Principles for the Governance of Outer Space Societies*, George Robinson, Issue 3:1 (Spring 1988)
- *Regulating International Trade in Launch Services*, Timothy Brooks, Issue 6:1 (Spring 1991)
- *Regulation of Alternative Operator Services*, Frank Darr, Issue 6:1 (Spring 1991)

S

- *Sales/Use Taxation of Software: An Issue of Tangibility*, John Kuo, Issue 2:1 (Spring 1987)
- *Scanning the Future of Copyrightable Images: Computer-based Image Processing Poses a Present Threat*, Benjamin Seecof, Issue 5:2 (Fall 1990)
- *Science and Toxic Torts: Is There a Rational Solution to the Problem of Causation?*, Susan Poulter, Issue 7:2 (Fall 1992)
- *Search for "Scientific Knowledge" in Federal Courts in the Post-Frye Era: Refuting the Assertion That "Law Seeks Justice While Science Seeks Truth," The*, Howard Denmark, Issue 8:2 (Fall 1993)
- *Secured Financing and Information Property Rights*, Raymond Nimmer and Patricia Krauthaus, Issue 2:2 (Fall 1987)
- *Semiconductor Chip Protection Act: Past, Present, and Future, The*, Steven Kasch, Issue 7:1 (Spring 1992)
- *Software Litigation in the Year 2000: The Effect of Object-Oriented Design Methodologies on Traditional Software Jurisprudence*, David Barkan, Issue 7:2 (Fall 1992)
- *Software Product Liability: Understanding and Minimizing the Risks*, Lawrence Levy and Suzanne Bell, Issue 5:1 (Spring 1990)
- *Sound Sampling Protection and Infringement in Today's Music Industry*, Molly McGraw, Issue 4:1 (Spring 1989)

T

- *Thinking Like a Lawyer: Expert Systems for Legal Analysis*, Richard Gruner, Issue 1:2 (Fall 1986)
- *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, Miles Feldman, Issue 9:1 (Spring 1994)

- *Transforming the Energy System: California's Plan to Develop Cogeneration*, William Manheim, Issue 2:1 (Spring 1987)

U

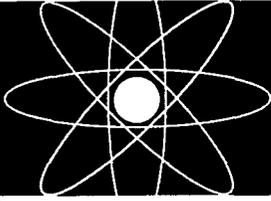
- *Uncertainty and the Standard of Patentability*, Robert Merges, Issue 7:1 (Spring 1992)
- *University Physician-Researcher Conflicts of Interest: The Inadequacy of Current Controls and Proposed Reform*, Claire Turcotte Maatz, Issue 7:1 (Spring 1992)
- *Use of Arbitration in Copyright Disputes: IBM v. Fujitsu, The*, Anita Stork, Issue 3:2 (Fall 1988)

V

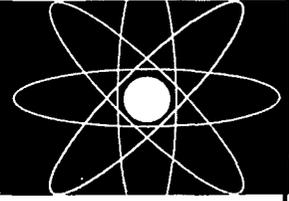
- *View From on High: Satellite Remote Sensing Technology and the Fourth Amendment, The*, Lisa Steele, Issue 6:2 (Fall 1991)

WXYZ

- *Watercloud Muddies the Water for Patent Coverage Disputes*, Howard Ross Cabot, Issue 8:2 (Fall 1993)



CALIFORNIA



ELEMENTS OF CONTROVERSY

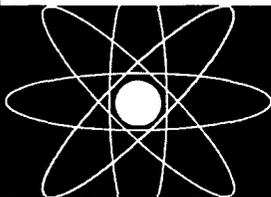
*The Atomic Energy Commission and
Radiation Safety in Nuclear Weapons
Testing, 1947-1974*

by **BARTON C. HACKER**

Despite these dramatic revelations important questions remain—the most controversial being: did the radiation overexposure in fact cause the cancers and birth defects for which it has been blamed? Hacker's work is the result of a decade of exhaustive research in AEC records and the full clinical and epidemiological literature on radiation effects. Although more concerned with uncovering the historical story than with assigning blame, the Department of Energy delayed publication of Hacker's study for five years.

Unforgettable congressional hearings in 1978 revealed that fallout from American nuclear weapons testing in the 1950s had overexposed hundreds of soldiers and other citizens to radiation. Faith in governmental integrity was shaken, and many people have assumed that such overexposure caused great damage.

\$55.00 cloth at bookstores or order toll-free 1-800-822-6657.



UNIVERSITY OF CALIFORNIA PRESS

