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

---

† 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 connotated 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 protocol[20] (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 C2[55] 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*, INFOWORLD, 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 RSA[87] 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 technology[92] 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/rslabs/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 cryptoanalysis 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 4I.

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 4I.

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.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. *FREEWARE 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 security[150] 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 Networld."[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").

plaintiff[163] 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 product[209] containing a dangerous defect[210] 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.*, Saloomey 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 software[215] 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 prostrate.[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); Ooooooooo (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. pmbl. (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 merchantable[278] 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 NCCUSL[304] 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 code[330] 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 rejection[343] 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 quality[353] and the implied warranty of system integration,[354] respectively. The proposed Article will probably create two other implied warranties, an electronic security warranty[355] 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 integration[357] 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 consumers[401] 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 contracts[445] 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 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]