THE TORT OF NEGLIGENT ENABLEMENT OF CYBERCRIME

By Michael L. Rustad† & Thomas H. Koenig‡

ABSTRACT

Michael L. Rustad and Thomas H. Koenig propose a new tort of negligent enablement which will hold software vendors accountable for defective products and services that pave the way for third party cybercriminals who exploit known vulnerabilities. At present, the software industry has externalized the costs of making code safe for its intended environment of use onto its end users through one-sided mass market agreements. The proposed negligent enablement tort fills the void left by the failure of contract law to give meaningful remedies for the unacceptably high levels of risk of computer intrusions due to defective software. The public policy rationale for imposing secondary tort liability on software publishers who aid and abet cybercriminals is to reduce the rate of cybercrime. The proposed negligent enablement tort draws upon well-established principles of the Uniform Commercial Code (UCC) Article 2 warranties, premises liability, and negligence-based product liability to construct a modified duty of care to produce safe software suitable for its environment of use. This Article examines the elements of duty, breach, causation, and damages for the proposed negligent enablement tort as well as defenses, procedure, and possible policy-based objections.

---

† Michael L. Rustad Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts.

‡ Professor Thomas H. Koenig chairs Northeastern University's Sociology and Anthropology Department and is on the Executive Committee of its Law, Policy & Society Doctoral Program.

We appreciate the editorial work and substantive suggestions of Chryss J. Knowles on this piece. Our research assistants, Shannon Downey, Kara Frato, John Hebb, and Conway Kennedy, worked diligently and creatively. Diane D'Angelo, a research librarian at Suffolk University Law School, provided us with extraordinary substantive assistance. Thank you also to the members of the Berkeley Technology Law Journal who contributed to the editing of this piece.

TABLE OF CONTENTS

I. INTRODUCTION

America is rapidly shifting its economic base from the production of durable goods to software engineering and other types of information production.[1] Since the 1990s, "the American economy [has] exploded with new technology and a proliferation of software and internet companies."[2] The total revenue of the top 500 software companies for 2004 was $330.7 billion, a 14% increase from 2003.[3] The interconnected nature of the internet is both its great strength and its Achilles heel.[4] The internet has spawned new classes of online injuries, such as the flood of spam e-mail and Trojan horse programs, that are choking electronic commerce and bilking unwary consumers.[5]

Highly vulnerable software often enables intruders to gain privileged access to computer systems, allowing intruders to alter code, compromise

1. This sea of change in the American economy is reflected in its shift from durable manufacturing to hardware and software manufacturing, internet sales and services, Computer-Aided Design (CAD), and Computer-Aided Manufacturing. Online computer databases, data processing services, and software publishing have displaced the assembly line. Software is at the heart of internet-based services such as call centers, electronic contracting, and online banking. The digitized image and computer graphics industry also rely upon software as do internet-related technologies such as multicasting. Computer software engineering is now a leading source of new jobs. Of the 675,000 software engineering jobs in 2002, 394,000 were computer applications software engineers. Another 281,000 Americans work as computer systems software engineers. U.S. Department of Labor, Bureau of Labor Statistics, Computer Software Engineers, http://www.bls.gov/oco/ocos267.htm (last visited Dec. 9, 2005).

2. Tanya Patterson, *Heightened Securities Liability for Lawyers Who Invest in Their Clients: Worth the Risk*, 80 TEX. L. REV. 639, 639 (2002).

3. John P. Desmond, *2004 Software 500: Growth Came in Segments*, SOFTWARE MAG.COM, Oct. 2004, *available at* http://www.softwaremag.com/L.cfm?Doc=2004-09/2004-09software-500.

4. "This profound integration of computers and information technology is obviously the strength of modern life, but it is also its vulnerability. The greater the vulnerability, the greater the ease with which it can be exploited." EDUARDO GELBSTEIN & AHMAD KAMAL, INFORMATION INSECURITY: A SURVIVAL GUIDE TO THE UNCHARTED TERRITORIES OF CYBER-THREATS & CYBER-SECURITY (2d ed. 2002), *available at* http://www.itu.int/wsis/docs/background/themes/security/information_insecurity_ed.pdf. Cybercriminals may easily exploit several vulnerabilities at the server level. *See* Michael L. Rustad & Lori Eisenschmidt, *The Commercial Law of Internet Security*, 10 J. OF HIGH TECH. L. 213, 216 (1995).

5. *See* Optinrealbig.com, LLC v. Ironport Sys., 323 F. Supp. 2d 1037, 1039 (C.D. Cal. 2004) (stating that approximately 80% of the e-mail received at AOL is spam and that $2 of each customer's monthly ISP fee is directed towards fighting spam).

personal data, or destroy system files.[6] Cisco's Authentication Proxy, for example, which is used in Cisco firewalls, contains a defect that hackers can exploit to execute viruses or other arbitrary code or to launch a denial-of-service (DOS) attack on an affected system.[7] Music publisher Sony BMG recently began releasing CDs containing anti-copying code, which caused software to be installed on users' computers without their knowledge or permission. The software contained a security vulnerability that hackers exploit to circumvent the user's firewall.[8] Defective software costs businesses and consumers tens of billions of dollars because of the large number of security vulnerabilities that enable cybercriminals.[9]

The first wave of computer security lawsuits stemmed from claims alleging that defective software offers inadequate security, and is unreliable in protecting network perimeters.[10] The race to market products without sufficient attention to quality results in software with known defects being released into the stream of commerce. As one software entrepreneur stated, "Everyone is in a dirty race to get products out quick, and they are getting their feet held to it on quality."[11]

A class action lawsuit was filed in San Francisco in July of 2005 against CardSystems Solutions, Inc., alleging that the company's lax computer security led to the wholesale misappropriation of credit and debit cards.[12] Committing one of the largest cybercrimes in world history, intruders gained unauthorized access to forty million credit cards and transfered data from 200,000 cards from CardSystems's computer network.[13] A

---

6. *See, e.g.*, United States Computer Emergency Readiness Team (U.S.-CERT), Cyber Security Bulletin, SB05-264, Summary of Security Items from Sept. 14 through Sept. 20, 2005, http://www.us-cert.gov/cas/bulletins/SB05-264.html.

7. U.S.-CERT Current Activity, Vulnerability in Cisco IOS Firewall Authentication Proxy, Sept. 8, 2005, http://www.us-cert.gov/current/current_activity.html.

8. *New Virus Uses Sony BMG Software*, CNN.COM, Nov. 10, 2005, http://www.cnn.com/2005/TECH/Internet/11/10/sony,hack.reut.

9. Quentin Hardy, *Saving Software From Itself*, FORBES, Mar. 14, 2005, at 60.

10. Gary H. Anthes, *The Future May Hold Bad Software, Ever-More-Dangerous Security Threats and a Host of Other Causes for Concern, Say Our Panelists*, COMPUTER WORLD, Mar. 7, 2005, at 36.

11. Hardy, *supra* note 9 (quoting Coverity's cofounder, Seth Hallem).

12. Complaint for Declaratory and Injunctive Relief, Parke v. CardSystems Solutions, Inc., No. CGC05-442624 (Cal. Super. Ct., July 5, 2005), *available at* http://www.techfirm.com/cardsystems.pdf [hereinafter CardSystems Complaint]; *see also* David Bank, *Security Breaches of Customers' Data Trigger Lawsuits*, WALL ST. J., July 21, 2005, at B1.

13. CardSystems Complaint, *supra* note 12, at 3; *see also* Joris Evers, *Judge Holds Off Disclosure in Credit Card Heist*, CNET NEWS.COM, Sept. 23, 2005, http://news.com.com/2100-7350_3-5879179.html.

California retailer and an individual plaintiff brought a class action suit against CardSystems Solutions, Inc. in California State Superior Court.

In the *CardSystems Solutions* litigation, the defendants were charged with negligent data security practices that allowed cybercriminals to compromise customers' credit card accounts.[14] The complaint charged CardSystems with numerous negligent acts, including insecure data handling practices, failure to maintain properly configured firewalls, failure to encrypt confidential customer data, and violations of reasonable internet security standards.[15] The complaint also charged the financial services firm with violating a California state statute requiring it to inform customers of computer intrusions that compromise their personal data.[16] CardSystem Solutions's class-action lawsuit is one of the first cases in which data handlers have been sued for negligent computer security practices.

At present, there is no available tort cause of action for producing software which enables breaches of computer security and highly foreseeable cybercrime. In the absence of tort liability, the software industry reallocates the costs of making its code safe for its intended environment of use to the end-user community. Customers receive a steady stream of releases, patches, updates, and new and improved security tools that they must install rather than rely upon a system that incorporates a comprehensive software security solution prior to release.[17] Critics charge that the software industry "would rather dump the security mess in the laps of users than solve it at the level where a solution really belongs: in the operating system, or the hardware, or the online provider's servers."[18]

This Article argues that a software vendor should be secondarily liable to consumers and other third parties for a new tort, namely the negligent enablement of cybercrime. Courts should recognize a modified duty of care on the part of software licensors to incorporate reasonable security into their products and services. Our proposed negligent enablement tort is premised upon the unacceptably high levels of risk of computer intrusions

14. CardSystems Complaint, *supra* note 12, at 3.

15. *Id.* at 2.

16. *Id.*

17. Walter Mossberg, *It's About Time For Somebody to Solve the Security Problem*, CHI. SUN-TIMES, Mar. 13, 2004, at 36.

18. Walter S. Mossberg, *PC Users Deserve a Free, Simple Service to Handle All Threats*, WALL ST. J., Mar. 11, 2004, at D1, *available at* http://ptech.wsj.com/archive/ptech-20040311.html.

caused by excessive preventable vulnerabilities in software.[19] The public policy rationale for imposing secondary liability on software publishers who aid and abet cybercriminals is to reduce the rate of malicious tortious or criminal activities. The software industry has simply abdicated to third parties its responsibility for limiting high-risk design defects. "The problem is that those responsible for securing our personal data are rarely the ones who pay the cost of securing it and in many cases are not the same people with whom we have entrusted our data in the first place."[20]

Our new tort of negligent enablement of cybercrime draws upon the Uniform Commercial Code's (UCC) well-established principles of warranties, premises liability,[21] and negligence-based product liability to construct a modified duty of care to produce safe software.[22] The negligent enablement tort will provide injured consumers and users with remedies when defective software paves the way for cybercrime. Part II of this Article documents the failure of contract law to provide software licensees with meaningful warranties and remedies for defectively designed code.[23] Presently, no recovery is available under contract law to redress the recovery of consequential damages caused by flawed software because courts

19. We use the term "defective software" to mean any software that fails to conform to its intended use in a substantial way. Defective software may take the form of bugs that lead to computational errors or inadequate security features that enable cybercriminals to misappropriate or alter data. Software failure may cause a computer to crash or function in a way that falls short of features that were warranted. *See generally* David Polin, *Proof of Manufacturer's Liability for Defective Software*, 68 AM. JUR. PROOF OF FACTS 3d 333 (2004).

20. Mark Rasch, *How Much Does a Security Breach Actually Cost?*, REGISTER, July 15, 2005, at 1, http://www.theregister.co.uk/2005/07/15/who_pays_for_security_breaches.

21. A premise liability lawsuit is "a claim for damages brought in civil court on behalf of a crime victim, usually against the owner of the premises where the crime occurred. The victim of a crime such as a mugging, assault, or rape seeks to hold the landowner responsible for the injuries—usually both physical and psychological—that the victim sustained, contending the crime was 'caused' by the landowner's failure to provide sufficient security to protect persons from criminal occurrences at the location." ALAN KAMINSKY, A COMPLETE GUIDE TO PREMISES SECURITY LITIGATION 3 (2d ed. 2001).

22. The concept of enabling liability for industries that facilitate third party crimes and other injuries to third parties was first developed in Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 452 (1999) (formulating negligent enablement cause of action against handgun manufacturers for marketing products "'inviting' misuse and consequent harm to innocent victims").

23. Steve Lohr, *Product Liability Lawsuits Are New Threat to Microsoft*, N.Y. TIMES, Oct. 6, 2003, at C2 (noting that the software industry has sidestepped the possibility of product liability by licensing software using agreements that disclaim warranties).

are unlikely to strike down one-sided liability-limiting license agreements. Part III reviews the social costs of insecure software, arguing that the greater the risk of enabling cybercrime, the greater the duty to protect the public. Part IV examines the elements of duty, breach, causation, and damages for the proposed new tort as well as defenses, procedure, and possible policy-based objections to recognizing negligent enablement. The tort of negligent enablement of cybercrime builds upon the bedrock principle of premises liability that those who aware of dangerous conditions but take no prompt remedial steps are liable for the consequences.

II. CONTRACT-BASED REALLOCATION OF DAMAGES

A. The Software Vendor's Blame Game

The recent increase of cybercrime shows no sign of abating, principally because the software industry has been slow to design comprehensive measures to protect against computer viruses. Forty-six major new computer infestations were recorded in 2004 versus only thirty-five virus epidemics in the previous year.[24] The security risk posed by dangerously defective software raises serious questions as to which party should bear legal responsibility for the consequences of cybercrime.

The software industry tends to blame cybercrime, computer intrusions, and viruses on the expertise and sophistication of third party criminals and on careless users who fail to implement adequate security,[25] rather than acknowledging the obvious risks created by their own lack of adequate testing and flawed software design.[26] Software licensers disavow responsibility for inadequate software even when their design decisions create systemic vulnerabilities.[27] This mistaken logic assumes that cybercrimi-

24. *Major Computer Viruses on the Increase***,** COMMC'NS & ELECS. REPORT, Jan. 25, 2005.

25. The software industry contends that assigning product liability would be unfair because software is "often misused or modified by consumers." *Id*. Software executives argue that expanded liability will have a chilling impact on innovation and undermine American competitiveness. Lohr, *supra* note 23, at 2.

26. *See* United States v. Ladish Mfg. Co., 135 F.3d 484, 488 (7th Cir. 1998) (discussing a defendant's ostrich-like approach to obvious risk).

27. *See* Jonathan Krim, *Security Report Puts Blame on Microsoft*, WASH. POST, Sept. 24, 2003, at E01 (quoting a Microsoft spokesman who states, "No other company in the world is more committed to providing its customers with more secure software than is Microsoft.").

nals are too skilled to be successfully thwarted, and therefore, that cybercrime is unavoidable—like death, natural disasters, and taxes.[28]

In reality, the blame for inadequate computer security must be shared between the software industry and the user community.[29] A distinguished panel of computer security experts concluded that "the deplorable quality of commercial software" has paved the way for an epidemic of cybercrime.[30] Sun Microsystems's Whitfield Diffie observed that many of the problems of computer security are due to bad software produced by firms that say, in effect, "'You pay. We promise you nothing. Have fun.' But we need to put in place legal targets—perhaps for 2010 or 2015—and improve our methodology to provide much higher security standards if we are to accept liability."[31] Software contracting law reallocates the cost of cybercrime by shifting legal responsibility from the designer to the user community.[32] In order to develop comprehensive solutions to the computer security problem, focus must shift from blaming cybercrime on customer inadequacies to the development of systematic, proactive solutions against malicious attacks by outside intruders.[33]

---

28. "It's obvious Microsoft doesn't bear 100% of the responsibility . . . but it's just as obvious that it doesn't bear 0%." Byron Acohido, *Hacker Victim Files Lawsuit Blaming Microsoft Security*, USA TODAY, Oct. 8, 2003, at 5B (quoting a representative of Counterpane Internet Security).

29. Krim, *supra* note 27, at E01 (citing report arguing that governments "should force Microsoft to reveal more of its software code to allow development of better security tools, and to make its software work better with competing products").

30. Anthes, *supra* note 10, at 36.

31. Shawna McAlearney, *Suing for Security*, INFO. SECURITY, Nov. 2003, at 16 (quoting Whitfield Diffie at the Information Security Solutions Europe event).

32. *See* Raymond T. Nimmer et al., *License Contracts Under Article 2 of the Uniform Commercial Code: A Proposal*, 19 RUTGERS COMP. & TECH L.J. 281, 294 (1993) (defining a "software contract" as "an agreement that transfers or promises to transfer one or more rights in specific computer software, including the right to access, the right to use or to have used, the right to modify, the right to copy or the right to otherwise employ the computer software").

33. *See* Tom Espiner, *Developers 'Should be Accountable' for Security Holes*, ZDNET UK, Oct. 12, 2005, http://news.zdnet.co.uk/software/developer/0,39020387,39228663,00.htm (arguing that software coders should be held liable for failing to develop secure applications); *Should We Blame Security Victims?*, Posting of Mike to http://www.techdirt.com/articles/20040428/0125258_F.shtml (Apr. 28, 2004, 01:29AM) (quoting security expert); *see also Frontline: Hackers* (PBS television broadcast), http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/giovagnoni.html (last visited Dec. 9, 2005) (interviewing Robert Giovagnoni, Executive Vice President for Strategic Relations for iDefense who observed that "liability [for computer intrusions] is a very real issue, and probably one of the greatest driving forces that we're going to be dealing with in the next few years").

Secure software,[34] proper firewalls, and computer security products have become highly profitable industries in their own right.[35] Companies that sell security solutions to industry have advocated reallocating the costs of defective software entirely to the manufacturer. For example, the CEO of Preventsys, Inc., a maker of enterprise security solutions calls for applying strict liability for third party losses resulting from insecure computer software or hardware.[36] Absolving end users from all responsibility for their own carelessness would be tantamount to absolute liability. Unlike strict liability, the negligence paradigm permits a sharing of responsibility for defective software that enables cybercrime.

The proposed negligent enablement tort will allocate responsibility to both software manufacturers and end users. Manufacturers will be held liable for marketing software with excessive preventable security flaws to vendors, but computer users will be accountable if they fail to protect passwords or take reasonable steps to implement vendors' security updates. Vendors that place software on the market with known vulnerabilities will also be liable for the consequences of excessive preventable risks. The next Section explores the industry's widespread use of one-sided adhesion contracts to reallocate the risks of defective software onto the user community. The development of a new negligent enablement tort will require software companies to build reasonable security into products and services through adequate testing.

---

34. Norton AntiVirus and McAfee AntiVirus are well-known examples of mass market security solutions. 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.

35. *See* George Myers, Jr., *Microsoft to Profit from Flaws in Windows*, COLUMBUS DISPATCH, Oct. 6, 2003, at 01C (describing Microsoft's plans to sell stand-alone antivirus software). In a 2004 study of the top 500 software companies, Symantec leads the security software category with $1.7 billion in sales, which was a 28% increase from 2003. Desmond, *supra* note 3.

36. Gene J. Koprowski, *The Web: Dealing with Cyber-Crime*, UPI, Feb. 16, 2005, *available at* http://www.upi.com/inc/view.php?StoryID=20050216-085340-1695r (quoting Tom Rowley).

B. Reallocating the Risks of Inadequate Computer Security

1. The Rise of Licensing Agreements to Reallocate Risk

The software industry was born when computer code was unbundled from hardware.[37] Computer vendors began selling hardware and licensing the use of software without conveying title.[38] The widespread licensing of software is emblematic of the transformation of a new information-based economy where access to software, data, and entertainment products outweighs the production of durable goods.

2. The Failure of Courts to Police the Software Industry

Mass market license agreements are classic examples of adhesion contracts in which the licensor routinely disclaims all meaningful warranties and remedies, and the manufacturer reallocates the risk of loss to the user community for all failures of performance.[39] The consumer is offered the product or service on a "take it or leave it" basis.[40] Many, even most, license agreements do not allow bargaining over any term or condition of service. Shrinkwrap agreements[41] and other mass market licenses typically

---

37. *The History of Computing: The Industrial Era*, Mar. 15, 2005, http://www.thocp.net/timeline/1978.htm (noting, for example, that the first business-type software, VisiCalc, was marketed in the 1970s and sold approximately a million copies); *see* MICHAEL D. SCOTT, INTERNET AND TECHNOLOGY LAW DESK REFERENCE 512 (1999); Bradford L. Smith & Susan O. Mann, *Innovation and Intellectual Property Protection in the Software Industry: An Emerging Role for Patents?*, 71 U. CHI. L. REV. 241, 243 (2004).

38. *See* Robert W. Gomulkiewicz, *Getting Serious About User-friendly Mass-Market Licensing For Software*, 12 GEO. MASON L. REV. 687, 689 (2004).

39. One-sided software license agreements are a form of adhesion contracts in which the weaker licensee submits to the terms of the licensor. *See generally* Frederich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

40. Shrinkwrap and other mass market license agreements are often presented to the user on a "take it or leave it" basis. David McGowan, *Free Contracting, Fair Competition, and Article 2B: Some Reflections on Federal Competition Policy, Information Transactions, and "Aggressive Neutrality"*, 13 BERKELEY TECH. L. J. 1173, 1213 (1998) (describing how proposed Article 2B validated software industry "take it or leave it" agreements); *see also* Michael L. Rustad, *Commercial Law Infrastructure For The Age of Information*, 16 J. MARSHALL J. COMPUTER & INFO L. 255, 300 (1997) (noting that mass market licenses are delivered to the user on a "take it or leave it" basis).

41. *See* David G. Post & Dawn C. Nunziato, *Shrinkwrap Licenses and Licensing on the Internet*, 477 PLI/PAT 517 (1997). Mass market licenses are often structured so that the consumer pays before having an opportunity to review the terms of the license agreement. The "pay now and see the terms later" approach to mass market licensing prevents consumers from shopping for more favorable terms. *See* Gomulkiewicz, *supra* note 38, at 716.

bind licensees to the terms of the dominant licensor without the possibility of negotiating key terms.[42]

The software licensor's purpose in issuing shrinkwrap license agreements is to create a "reverse unilateral contract,"[43] which is structured so that the customer who opens the plastic wrap and uses the software will be bound to one-sided terms.[44] "One can read hundreds of click-wrap, Web site, shrink-wrap, and other mass-market transactions and have yet to find a single example of a software licensor willing to provide any warranty for its software."[45] A pundit wryly observed that "by unwrapping a software package or downloading a demo, you've agreed to a thickly worded contract that may result in enslaving your first-born child to Bill Gates for all you know."[46]

Licensors typically disclaim warranties, offering only the repair or replacement of the software disk or other media as the sole and exclusive remedy.[47] The typical "click through" website agreement requires end users to click on an icon, "I agree," which creates a contract where the user agrees to submit to all of the licensor's terms and conditions. For example, Dell's software agreement binds the consumer to all the terms of its license agreement when the preloaded software is used.[48]

---

42. Software publishers impose standard one-sided terms in the typical shrinkwrap agreement. *See* Batya Goodman, Note, *Honey, I Shrink-Wrapped the Consumer: The Shrink-Wrap Agreement as an Adhesion Contract*, 21 CARDOZO L. REV. 319 (1999) (documenting the widespread industry practice of software publishers offering standard terms to the user community).

43. Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1241 (2000).

44. *Id*.

45. Michael L. Rustad, *Making UCITA More Consumer-Friendly*, 18 J. MARSHALL J. COMPUTER & INFO. L. 547, 579 (1999) (arguing that UCITA should be amended to incorporate greater consumer protection for licensees).

46. *Id.* at 578 (quoting Margie Wylie, software critic). A famous Dilbert cartoon lampoons adhesive shrinkwrap license agreements, by forcing Dilbert to become Bill Gates' towel boy. Scott Adams, *Dilbert*, RICHMOND TIMES DISPATCH, Jan. 14, 1997, at D5. For a discussion of how software vendors developed restrictive license agreements for packaged software, see Rustad & Eisenschmidt, *supra* note 4, at 267-93.

47. *See, e.g.*, i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 329, 334 (D. Mass. 2002) (describing the ubiquity of mass market license agreements where the user manifests assent by clicking "I Agree" and thereby creating an enforceable agreement to limit liability).

48. Dell USA, Dell Software License Agreement, http://www1.us.dell.com/content/topics/global.aspx/policy/en/policy?c=us&l=en&s=gen&~section=015 (last visited Nov. 11, 2005) (stating terms of the software agreement between Dell Products, LP and its customers).

One-sided choice of law[49] and forum selection clauses[50] have a chilling effect on the user's ability to file suit for defective software. It is prohibitively expensive, for example, for a Minnesota consumer to file suit in Washington, the forum chosen by Microsoft. Requiring a consumer to file suit in a distant forum functions as an absolute immunity, where the cost and inconvenience of filing a lawsuit far exceed what can be recovered if they prevail. Very few consumers are even aware that they waive their implied warranty of merchantability, surrender their right to file suit in a court of law, and agree to submit to arbitration in a distant forum by the mere act of clicking on an icon labeled "I agree."[51] It is questionable whether most consumers even understand that they are typically licensing, not purchasing, software.

A license conditions access to and use of software on acceptance of the license's terms.[52] A mass market agreement generally begins with a legal notice, disclaimer, or terms of use, stating that opening the package indicates the users' acceptance of the license terms.[53] The license agreement is

---

49. *See* Jeffrey D. Dunn, *Texas Choice of Law Analysis for Contracts*, 40 TEX. J. BUS. L. 37, 39 (2004) (describing choice of law and conflicts of law analysis).

50. The U.S. Supreme Court in Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991) enforced an onerous forum selection clause of a cruise contract requiring the consumer to litigate in Florida, a forum distant from the consumer. *See also* Net2phone, Inc. v. Superior Court, 109 Cal. App. 4th 583, 588 (2003) (citing *Carnival Cruise* as authority for a "take it or leave it" forum selection clause). Courts have frequently required users to litigate in distant forums since the advent of the internet. *See, e.g.*, CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Westendorf v. Gateway 2000, Inc., 41 U.C.C. Rep. Serv. 2d (CBC) 1110 (Del. Ch. 2000) (holding that the plaintiff was bound to an arbitration clause because she kept her computer for thirty days, thereby accepting Gateway's terms and conditions for sale of the computer and related services). *But see* Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002) (refusing to enforce choice of forum clause where license agreements were located on a submerged screen that the user would have needed to scroll through to read the full agreement and arbitration clause, and holding therefore that the internet users' act of downloading the software did not unambiguously manifest assent to the arbitration provision in the license terms).

51. A typical software license agreement for a computer security product disclaims all express and implied warranties including fitness for a particular purpose and non-infringement of third party rights. Products are offered on an "as is" or "without any warranties of any kind" basis, that do not even warrant functionality of the product without defect or vulnerability. *See, e.g.*, Lockdown Networks, End User Software License Agreement, http://www.lockdownnetworks.com/freeaudit/conditions.php (last visited Sept. 25, 2005).

52. *See, e.g.*, Real Networks, Legal Notice Disclaimer and Terms of Use, http://www.realnetworks.com/company/legal.html (last visited Dec. 2, 2005).

53. For example, Adobe Systems provides that the customer's downloading of software from its website signifies agreement to its terms and conditions. Adobe, Downloads, http://www.adobe.com/support/downloads/main.html (last visited Dec. 2, 2005).

frequently not even visible to a consumer before purchase because it is sealed inside the product's packaging.[54] Mass market license agreements not only reallocate the risk of software failure[55] to the licensee, but usually also bypass the first sale doctrine of federal copyright law.[56]

Prior to the mid-1990s, U.S. courts were reluctant to enforce adhesion contracts in the form of software agreements.[57] However, the courts' attitudes have since changed in favor of broad enforceability of mass market license agreements; the current trend is to enforce one-sided software agreements so long as the user has an opportunity to review and manifest assent to the terms.[58] In *ProCD*,[59] the Seventh Circuit upheld the enforceability of a shrinkwrap license located inside the package of the computer program. The bargaining power of the parties with respect to the mass market agreement was highly unbalanced, in part because consumers were not able to see the terms of the contract until after the software was purchased. The court summarily rejected the licensee's claim that he had no choice but to adhere to the licensor's terms once he opened the package[60] and gave short shrift to the argument that shrinkwrap licenses must be conspicuous to be enforceable.[61] The court found that the licensor invited

---

54. *See, e.g.*, Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) (enforcing license agreement with clause ordering arbitration despite the fact that the agreement was not available to the consumer prior to purchase).

55. *See* Daniel T. Perlman, Note, *Who Pays the Price of Computer Software Failure?*, 24 RUTGERS COMPUTER & TECH. L.J. 383, 387 (1998) (defining software failure as "the occurrence of either deficient functionality, where the program fails to perform a required function, or deficient performance, where the program performs a required function too slow or in an insufficient manner").

56. The first sale doctrine of copyright law gives the owner of a lawfully made copy the power to "sell or otherwise dispose of the possession of that copy without the copyright holder's consent." Step-Saver Data Sys. v. Wyse Tech., 939 F.2d 91, 96 n.7 (3d Cir. 1991) (quoting Bobbs-Merrill Co. v. Straus, 210 U.S. 339, 350 (1908)).

57. *See, e.g.*, Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255 (5th Cir. 1988) (affirming a district court finding that a shrinkwrap license was an unenforceable adhesion contract and ruling that federal copyright law preempted Louisiana's Software License Enforcement Act); *Step-Saver Data Sys.*, 939 F.2d at 105 (ruling that box-top mass market license was an additional term not incorporated into the parties' contract where the term's addition to the contract would materially alter the agreement and the consumer did not see the license until after paying for product).

58. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (upholding a shrinkwrap license); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000) (upholding a limitation on consequential damages included in a license accompanying protection devices for mass market software).

59. 86 F.3d at 1447.

60. *Id.*

61. *Id.* at 1452.

acceptance by silence and that the licensee accepted the software after having an opportunity to reject its terms.[62] In so holding, the Seventh Circuit validated the software industry's practice of disclaiming all warranties and all meaningful remedies, reasoning that this form of licensing benefited consumers by permitting them to make extra copies, use software on multiple computers, and incorporate software into the user's own products.[63] In *Hill v. Gateway*,[64] the same court further extended its pro-industry tilt by ruling that a customer was bound by an arbitration clause contained in the packaging of a computer, regardless of whether it was conspicuous or if the purchaser had actual knowledge of its existence.

As demonstrated in previous cases, the evolution of software law has led to the enforcement of unsigned adhesion contracts, depriving consumers of meaningful remedies.[65] The Uniform Computer Information Transactions Act (UCITA), the first comprehensive statute for software licensing, is a model act which also represents a pro-licensor standpoint by its validation of one-sided mass market license agreements.[66] In sum, contract law has failed to provide consumers and other users with meaningful remedies to redress foreseeable cybercrimes caused by defective software design. In the absence of adequate contractual remedies for defective software, corporate users must purchase specialized insurance policies to cover risks that should be borne by the software manufacturer.

In the next Part, we propose the expansion of tort remedies to redress the financial costs of cybercrime enabled by defective software. We argue that courts should examine public policy interests as well as precedent in determining whether to recognize a new duty or modify an old one.[67]

---

62. *Id.*

63. *Id.* at 1455.

64. 105 F.3d 1147 (7th Cir. 1997).

65. *See, e.g.*, *ProCD*, 86 F.3d at 1450 (validating license agreement and treating licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the UCC); i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002) (relying on U.C.C. § 2-204 to validate a clickwrap license agreement); Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 571-72 (App. Div. 1998) (holding that assent to shrinkwrap agreement occurred in consumer's actions after time of purchase instead of at purchase).

66. *See* Rustad, *supra* note 45, at 547 (arguing that UCITA should be amended to extend federal and state consumer protection to mass market license agreements).

67. *See* Robert L. Rabin, *The Torts History Scholarship of Gary Schwartz: A Commentary*, 50 UCLA L. REV. 461, 480 (2002).

III. TOWARDS A DUTY OF CARE TO PRODUCE SECURE SOFTWARE

This Part argues that courts should recognize a duty of software vendors to market software with reasonably secure software to prevent cybercrime. Consumers and licensees have been left without meaningful warranties or remedies for software failure. To date, despite an epidemic of computer security flaws, no plaintiff has recovered damages for cybercrimes enabled by flawed software under either a contract theory or under a tort theory. Most software security incidents result from hackers exploiting known vulnerabilities arising out of grossly inadequate software engineering practices.[68] Too many vendors market their products and services with vulnerabilities that improved software development practices could reduce.[69]

Software vendors, not computer users, are in the best position to design software that deters cyber-intruders. Software defects should be detected by software engineers before a product's release. Furthermore, software vendors can bundle together tools to prevent foreseeable cybercrimes. For example, vendors possess technology to track antivirus software and to warn users if their protection is not installed or properly updated.[70] The social costs associated with hackers, viruses, and cybercrimes will not decrease until the software industry is held accountable for marketing products with known design defects. Constructing a duty of care to produce secure software will provide vendors and other stakeholders incentives to implement, install, and update safe and reliable products and

---

68. Noopur Davis, *Developing Secure Software*, SOFTWARE TECH NEWS, July 2005, at 3, 3, *available at* http://www.softwaretechnews.com/stn8-2/noopur.html ("Most security vulnerabilities result from defects that are unintentionally introduced in the software during design and development. Therefore, to significantly reduce software vulnerabilities, the overall defect content of software must be reduced."). "Almost all software is riddled with holes, and programs are released to purchasers with hundreds, if not thousands, of security-related weaknesses." Reid Skibell, *The Phenomenon of Insecure Software in a Security-Focused World*, 8 J. TECH. L. & POL'Y 107, 108 (2003) (citing Bruce Schneier, *Foreword* to JOHN VIEGA & GARY McGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY, at xix (2002) ("[T]he average large software application ships with hundreds, if not thousands, of security related vulnerabilities")).

69. *Id*.

70. Tom Mainelli, *Internet Security Suites Face Off*, PC WORLD, Feb. 2005, at 50-51.

services.[71] Robust internet security constitutes the first line of defense against spam, viruses, and other cybercrimes.

The courts have yet to articulate such a duty of care for software manufacturers.[72] Recently, however, plaintiffs have asserted such a duty. Class action suits against Reed-Elsevier's LEXIS/NEXIS and ChoicePoint Inc. were filed in federal district courts in California for failing to implement security that might have prevented the theft of customers' personally identifiable information.[73] The Federal Trade Commission entered into a consent agreement with BJ's Wholesale Club Inc.,[74] whose customers' credit card information was compromised by computer hackers.[75] In the agreement, BJ's agreed to develop a comprehensive plan to protect the security of their customers.[76]

These computer security cases may signal a greater willingness of courts to recognize a duty to implement reasonable software security practices.[77] Should courts recognize this duty, software vendors should expect

---

71. [A] court's task in—determining 'duty'—is not to decide whether a particular plaintiff's injury was reasonably foreseeable in light of a particular defendant's conduct, but rather to evaluate more generally whether the category of negligent conduct at issue is sufficiently likely to result in the kind of harm experienced that liability may appropriately be imposed on the negligent party.

Ballard v. Uribe, 41 Cal. 3d 564, 573 n.6 (1986) (emphasis omitted).

72. *See* Jonathan B. Mintz, *Strict Liability for Commercial Intellect*, 41 CATH. U. L. REV. 617, 649 (1992); Stephen E. Henderson & Matthew E. Yarbrough, *Frontiers of Law: The Internet and Cyberspace: Suing the Insecure? A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 15 (2002) (noting that there is little authority for extending a duty of care to internet security threats). Some commentators have urged that strict liability not be extended to software because of the chilling effects on innovation. Donald R. Ballman, *Software Tort: Evaluating Software Harm by Duty of Function and Forum*, 3 CONN. INS. L.J. 417, 421 (1996-1997).

73. *Ballard*, 41 Cal. 3d at 573 n.6.

74. Credit unions and their insurers filed suit against BJ's and its bank on fraud, negligence, and other grounds, seeking to recover the cost of closing accounts and reissuing cards. Bank, *supra* note 12, at B8.

75. *Id.* at B1.

76. The consent order agreed to by BJ's Wholesale Club bound the corporation and all its subsidiaries or divisions, "in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service" to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." *In re* BJ's Wholesale Club, FTC Order #0423160, http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf (last visited Dec. 2, 2005).

77. "[T]he software industry is no longer in its infancy. Its development has moved out of garages and into corporate offices. It has matured to become a dominant sector of

a "flood of lawsuits by both consumers and businesses" stemming from breaches of data security.[78] A special advisor to President Bush opined that reform will come through litigation: "We'll see [venders] getting sued [because] so much of our infrastructure depends on computers that it's unsustainable to hold software companies blameless."[79]

Just as landowners who open their premises to business visitors owe a duty of care, the software industry may be required by an expansion of tort law to use reasonable precautions to protect its users from computer intruders.[80] Several new torts emerged during the twentieth century to remedy the previously "unredressed harms of intentional infliction of emotional distress, invasion of privacy, product-related injury, and wrongful discharge."[81] Our proposed negligent enablement tort, like these other innovations in tort law, "is not so much a new creation as an adjustment to well-established law,"[82] based upon professional malpractice, product liability, and premises liability. While each of these legal theories would need considerable modification before being extended to software transactions, they serve as useful heuristic devices for visualizing the contours of the new enablement tort. The negligence-based enabling tort anchors li-

---

the economy. Consequently, it is appropriate to consider liability for defective software in the same light as liability for defective automobiles, pharmaceuticals, and other products." Frances E. Zollers et al., *No More Soft Landings for Software, Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 746 (2005); *see also* Mark Jewell, *Credit Fraud Raises ID-Theft Concerns*, THE CALL, July 5, 2004, *available at* http://www.zwire.com/site/news.cfm?newsid=12215347&BRD=1712&PAG=461&dept_id=24361&rfi=6%20.

78. Bank, *supra* note 12, at B1 (quoting Mark Rasch, Senior Vice President for Solutionary, Inc.).

79. Neville Smith, *Insurers May be Hit by A Bad Idea Whose Time Has Come: Class Actions Over Faulty Software Could Land Insurers in a Tangle*, LLOYD'S LIST INT'L , Sept. 23, 2004, at 6.

80. *See* DAN B. DOBBS, THE LAW OF TORTS 876 (2001). In addition to the landowner's duty to protect customers, there are a large number of relationships between a defendant and the plaintiff where the duty to use reasonable care against third party criminals is based upon the superior party's relationship to the plaintiff. A duty to protect the plaintiff from third party intrusions is present in the formal relationship between common carrier and passenger, parent and child, schools and students, and employers and employees. *Id*. at 874-75.

81. Anita Bernstein, *How to Make a New Tort: Three Paradoxes*, 75 TEX. L. REV. 1539, 1541 (1997) (explaining how new causes of action evolved).

82. *Id*. at 1555 (arguing that new torts such as the invasion of privacy, the intentional infliction of emotional distress, wrongful termination, and product liability only survived because they were "framed" in terms of well-established, as opposed to novel, victim classes).

ability to accepted industry standards, federal and state community security statutes, and risk/utility formulas.

Under our proposed negligent enablement tort, the software industry would owe its users an affirmative duty of reasonable care in protecting them from highly foreseeable cybercrime by eliminating negligent design practices, inadequate internet security services, and poorly configured firewalls. The allocation of software liability should attach where the industry fails to implement available means to prevent foreseeable cybercrimes.[83] Just as in premises liability cases, courts should impose negligence-based liability for failure to implement available means to protect software customers from third-party crimes. Although courts are unlikely to stretch landowner's duties to apply to cyberspace, customer protection from acts by foreseeable third-party criminals is functionally equivalent.[84] Similarly, although courts are unlikely to expand the principles of strict product liability to software, software vendors are best suited to maintain proper computer security.

In a networked world, it is reasonably foreseeable that computer hackers or cybercriminals will discover and exploit known vulnerabilities in operating systems. The number of security breaches experienced by software consumers has reached epic proportions.[85] Such errors cost the U.S. economy an estimated $59.5 billion each year.[86] In addition, dangerously

---

83. Defective software creates widespread harm because "[t]he software industry [is] one of the most important sectors of the economy. Performance gains in computer hardware, advances in software functionality, and the growth of the Internet into an established communications and commercial medium have fueled the integration of software into nearly every aspect of modern life." Smith & Mann, *supra* note 37, at 241.

84. The salutary trend of the law has been to impose a duty of care on landowners for preventing third-party crimes. DOBBS, *supra* note 80, at 876. This duty has been extended to common carriers, operators of hotels, theaters, and places of public entertainment. *Id.*

85. The CERT Program of the Software Engineering Institute (SEI) of Carnegie Mellon University was established by the U.S. Department of Defense as an Advanced Research Project to coordinate computer security emergencies, analyze computer software vulnerabilities, and develop security solutions. CERT Coordination Center monitors computer and cyber security and develops techniques to survive and resist attacks on computer systems. SEI, Meet CERT, http://www.cert.org/meet_cert/meetcertcc.html#bkgd (last visited Sept. 26, 2005). In a six month period, the CERT Coordination Center at Carnegie Mellon University received over half a million e-mails and nearly one thousand calls reporting computer security incidents or requesting information. The Center handled 137,529 computer security incidents during this period. SEI, CERT Coordination Center 2003 Report, http://www.cert.org/annual_rpts/cert_rpt_03.html#highlights.

86. Alia Susann Zohur, Comment, *Acknowledging Information Technology Under the Civil Code: Why Software Transactions Should not be Treated as Sales*, 50 LOY. L. REV. 461, 461 (2004).

defective software enables other thefts, such as the theft of credit card information, trade thefts, and the interception of personally identifiable data.[87] Any data handler or software licensor should be liable for losses resulting from the marketing of software with inadequate security features.[88]

Software publishers releasing dangerously insecure code should shoulder the costs of enabling foreseeable computer intruders. For the software industry to incur liability for negligently causing harm, the vendor must owe a duty of care to its licensees. Judicial opinions in negligence cases demonstrate that determinations of no duty are rare.[89] A company will have a duty where its conduct poses preventable risks to others.[90] Such a duty may arise from a company's failure to anticipate tortious or criminal acts of others, although "courts are reluctant to impose a duty to anticipate the criminal or tortious conduct of third parties."[91]

The limited duty would require the licensors of network security and mass market products to implement computer code that is reasonably fit for their intended environment of use. In software law, as in any other area of tort law, the greater the risk, the greater the duty of care. The software vendor's duty to protect third party personal and proprietary information should be calibrated by the radius of the risk. A software vendor that markets tailored software to a hospital or to a financial institution, for example, would have a higher duty of care to produce secure software than a vendor marketing to the home entertainment market.

The marketing of software or network services without adequate perimeter defenses provides, in effect, a welcome mat for hackers, crackers,[92] and other cybercriminals. Microsoft's Internet Explorer has become

---

87. The most common software defects enabling computer intrusions include: buffer overflows, format string problems, SQL injection, command injection, failure to handle errors, cross-site scripting, failing to protect network traffic, the use of "magic" URLs and hidden forms, improper use of SSL, use of weak password-based systems, failing to store and protect data, information leakage, improper file access, integer range errors, trusting network address information, signal race conditions, unauthenticated key exchange, failing to use cryptographically strong random numbers, and poor usability. Michael Howard's Web Log, The 19 Deadly Sins of Software Security, http://blogs.msdn.com/michael_howard/archive/2005/07/11/437875.aspx. (last visited Dec. 9, 2005).

88. *See* Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability & the First Amendment*, 24 WHITTIER L. REV. 71, 131 (2002).

89. *Id*.

90. *See* Rabin, *supra* note 67, at 480.

91. *Id.*

92. A cracker is generally defined as a "hacker with criminal intent." Eric J. Sinrod & William P. Reilly, *Cyber-crimes: A Practical Approach to the Application of Federal*

an instrumentality of choice for cybervillains to spread internet worms via online advertisements.[93] Computer "intruders have become highly proficient at turning internet-connected Windows PCs into obedient 'zombies.'"[94] When software vendors provide antivirus, firewall, spam, spyware, patches, and other post-marketing stop-gaps for computer security, it is like using "chewing gum stuck in the cracks of a sinking ship."[95] A comprehensive security solution is needed to thwart crime.

The next Section contends that a duty of care must be recognized given the radius of the risk of cybercrime caused by defectively designed software. If the vendors are held liable for the consequences of defective software, they will have a strong incentive to develop comprehensive solutions for thwarting cybercriminals, instead of continuing with the current "perimeter centric model" of focusing too narrowly on strengthening borders through improved firewalls.[96]

A. The Radius of the Risk of Defective Software

The number of detected software vulnerabilities has increased rapidly over the past decade. Figure 1 below illustrates this steady increase of known software flaws. Given that corporations are reluctant to report that their security has been breached, the number of detected vulnerabilities is likely even greater than depicted in Figure 1.[97] In addition, the Federal Trade Commission estimated in 2003 that personal data from approximately ten million Americans was stolen that year, resulting in

---

Computer Crime Laws, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 182 (2000). Cracking is defined as "computer system 'break-ins' to secure computer services and computer-storage such as databases of credit-card details." Roger Clarke, *Paradise Gained, Paradise Re-lost: How the Internet is being Changed from a Means of Liberation to a Tool of Authoritarianism*, 18 MOTS PLURIELS, Aug. 2001, at sec. 3.2, *available at* http://www.anu.edu.au/people/Roger.Clarke/II/PGPR01.html.

93. Stuart J. Johnston, *Protect Your Browser From Attack Ads*, PC WORLD, Feb. 2005, at 47 (describing malicious code as exploiting an operating systems defect in Windows 98 and XP versions of Microsoft's program).

94. *The Rise of Zombie Computers*, USA TODAY, Sept. 8, 2004 at 3B.

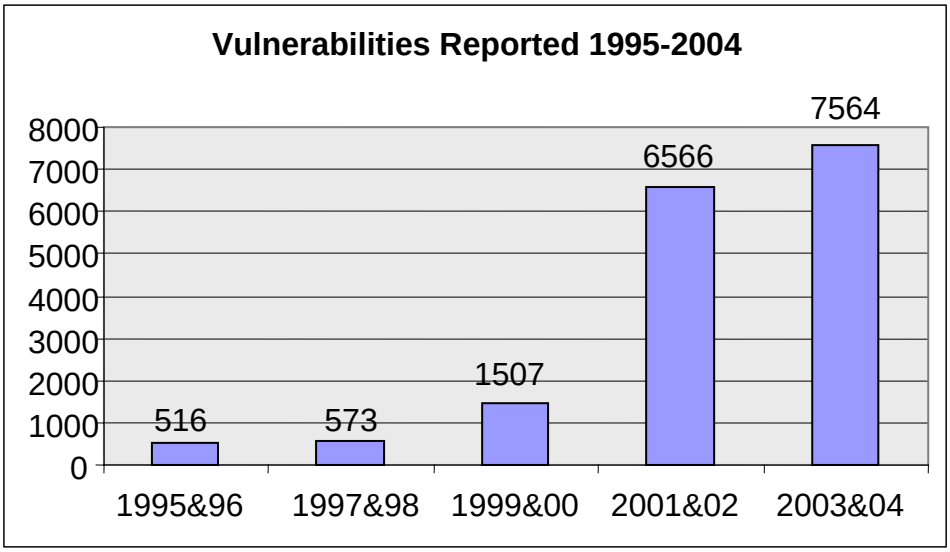
95. John Dix, *How the Bad Guys View Software*, NETWORK WORLD, Mar. 8, 2004, at 38 (quoting a question presented to computer security expert Gary McGraw).

96. Erik Pace Birkholz, *Birkholz Fights Network Negligence at Inland Empire ISSA*, PR WEB DIRECT, June 28, 2005, http://www.prwebdirect.com/releases/2005/6/prweb256232.htm.

97. The underreporting of cybercrime intrusions is likely the result of a company's desire to avoid undue publicity or the loss of public confidence because of its inability to prevent intrusions.

direct losses of $5 billion to consumers and another $48 billion in losses to the business community.[98]

Figure 1: The Growth in Software Defects[99]



Security holes are not rare anomalies; rather, they have become the software industry norm. Spyware entrepreneurs commonly exploit security holes to install unwanted software such as pornographic icons on users' computers.[100] For example, employees at AOL, the world's largest internet

98. Press Release, FTC, FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers (Sept. 3, 2003), *available at* http://www.ftc.gov/opa/2003/09/idtheft.htm.

99. The historical data on vulnerabilities reported in Figure 1 is constructed from reports to the CERT Coordination Center (CERT/CC), which is a federally funded center located at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, Pennsylvania. *See* SEI, CERT/CC Statistics 1988-2005, *available at* http://www.cert.org/stats/cert_stats.html.

100. The vendors of unwanted software and spam use at least four methods to install software on personal computers without obtaining the computer users' informed consent: (1) drive-by downloads; (2) installation via distribution partners; (3) installation through security holes; and (4) installation at a user's request without displaying a license agreement. Ben Edelman, 180solutions Installation Methods and License Agreement, http://www.benedelman.org/spyware/180-affiliates/installation.html (last visited Dec. 8, 2005). The modus operandi of a "drive-by download" is to send misleading pop-up offerings to install software while the user is browsing. The user may inadvertently install software without even seeing the terms and conditions of the license agreement. *Id.*

service provider, accidentally downloaded virus-infected e-mails leading to the compromise of the system.[101]

Windows software contains multiple vulnerabiltiies that enable malicious users to obtain elevated privileges, gain arbitrary file access, or execute arbitrary code.[102] For example, security holes in Microsoft's Internet Information Server permit malicious code to be installed on a user's computer.[103]

An empirical study of thousands of software programs documented the lax practices in the design, coding, and testing of software that leads to vulnerabilities.[104] The researchers found approximately one coding error for every seven to ten lines of new and changed software.[105] Even if 99% of these errant codes were detected and removed, the rate of error would be unacceptably high.[106] To change this systematic pattern of insecure software design, computer security must be built into each phase of the product development cycle. The current haphazard approach, in which security is "bolted-on" after a vulnerability is discovered in the post-marketing period, creates too many social costs.[107]

One of the earliest computer security breach lawsuits was filed against Microsoft in 2003 for marketing software with known security vulnerabilities.[108] The plaintiff's complaint charged Microsoft with unfair competition, violation of California's unfair and deceptive trade practices law, and violation of a state law requiring notification of security breaches.[109] The underlying factual claim is that Microsoft knowingly marketed its soft-

---

101. Jim Hu, *AOL Security Breach Exposes Personal Info*, CNET NEWS.COM, June 16, 2000, http://news.com.com/2100-1023-242034.html?legacy+cnet. ("AOL, the largest Internet service provider with 23 million paid subscribers, is targeted frequently by account crackers.").

102. *See* Who Profits from Security Holes?, http://www.benedelman.org/news/111804-1.html (Nov. 24, 2004).

103. *Id.*; *see also* Preston & Lofton, *supra* note 88, at 73 (explaining the buffer overflow vulnerability created by security holes in Microsoft's Internet Information Server).

104. *See* Davis, *supra* note 68 (reporting results of an SEI study and arguing that "[m]ost security vulnerabilities result from defects that are unintentionally introduced in the software during design and development").

105. *See id.*

106. *See id.*

107. *Id.*

108. Class Action Complaint, Hamilton v. Microsoft Corp., No. 49-031017-1010 (Cal. Super. Ct. Sept. 30, 2003) (charging Microsoft with launching numerous products with security flaws enabling cyberattacks, viruses, worms, and Trojans).

109. *Id*. at 11-12.

ware despite knowing of defects that permitted widespread identity theft[110] and the possibility of cascading failures in computer systems.[111] To date, no third-party victim of inadequate computer security has received a single dollar of compensation in any contract or tort-based lawsuit.

B. Lessons Learned from New Tort Duties

During the second half of the nineteenth century, tort law evolved to protect the public against new dangers arising from the dramatic expansion of industrial enterprises. Negligence emerged as the liability standard for non-intentional injuries caused by railroads, streetcar companies, and industrial corporations.[112] During this era, tort law was characterized by a host of defenses, immunities, and special privileges that limited the liability of corporate defendants.[113]

After World War II, the reach of tort law expanded to counter new social hazards created by the rapid growth of corporate, medical, and governmental bureaucracies. Prior to the 1960s, manufacturers were shielded from liability by the doctrine of privity and other barriers to recovery. Strict product liability assigned losses based, in part, upon the public policy recognition that the manufacturer is in the best position to avoid the perils of defective products. The expansion of tort liability to govern bad software may be more efficient than a rigid regulatory regime.[114]

The recognition of a negligent enablement duty will impose short-term costs on the software industry because of the need to institute preventive law audits and other quality measures for each of the design and testing

---

110. Computer intrusions frequently result in identity theft because a cybercriminal or intruder steals information such as Social Security numbers, credit card information, or bank account information to complete fraudulent transactions.

111. *Id.*

112. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 3 (Proposed Final Draft No. 1, Apr. 6, 2005) (discussing basic principles of negligence). The Restatement defines negligence as the failure to exercise the standard of reasonable care. *Id.* We believe the variables of foreseeability of harm, severity of harm, and the burden of precaution apply equally well to software vendors or manufacturers. In the context of insecure software cases, we argue the vendor should be held negligent based upon marketing products or services where there was a high foreseeability of harm with readily available means "to eliminate or reduce the risk of harm."

113. *See* Robert L. Rabin, *The Historical Development of the Fault Principle: A Reinterpretation*, *in* PERSPECTIVES ON TORT LAW 44, 68 (Robert L. Rabin ed., 2d. ed. 1983). "The term 'privilege' has come to be regarded as a general purpose of social policy in the law of torts." FOWLER HARPER, A TREATISE ON THE LAW OF TORTS 51 (1933).

114. *See* Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 373 (1984).

stages. However, these costs will ultimately be borne by the user community as will the cost of litigation and insuring these new liabilities.

Software vendors contend that imposing greater liability on the industry is impractible because one cannot create defect-free software. Furthermore, it will stifle innovation and punish the wrong entity.[115] However, even the corporate community acknowledges that legal liability often results in superior products. The business-backed Conference Board reported:

> Where product liability has had a notable impact—where it has most significantly affected management decision-making—has been in the quality of the products themselves. Managers say products have become safer, manufacturing procedures have been improved, and labels and use instructions have become more explicit.[116]

While no software can be totally bulletproof, the current legal regime misses the mark by too wide a margin. Slipshod software testing gives a competitive advantage to the developer who releases poorly tested software whose vulnerabilities will be discovered only after the user is harmed.[117] A balance must be found that allows responsible software sellers to continue to thrive while protecting the legitimate security interests of the computer user.

1. Product Liability for Defective Software

Product liability refers to the liability of manufacturers, processors, distributors, and sellers of products for personal injury or property damage under diverse theories including: negligence, strict liability, and breach of warranty.[118] Product liability in a bad software case would be based upon

---

115. Bruce Schneider, *Should Vendors be Liable for Their Software's Security Flaws?; Two Industry Leaders Debate Whether Vendors Should be Accountable for Vulnerable Products*, NETWORK WORLD, Apr. 22, 2002, at 51.

116. NATHAN WEBER, CONFERENCE BOARD, PRODUCT LIABILITY: THE CORPORATE RESPONSE 14 (Rep. No. 893, 1987).

117. Imposing product liability on software vendors will shift the cost of precaution onto those vendors through increased cost for improved testing, research, and beta testing of software before releasing it into the market. Although substantial, these costs will be less than the duplicative costs of requiring every computer user to secure every computer system with a patch and assume the consequences of not taking this remedial measure. It is more cost-efficient for software licensors to take precautions prior to marketing software than requiring the user to take remedial steps in the post-marketing period. *See* Preston & Lofton, *supra* note 88, at 134.

118. THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 35, 51-59 (2001) (explaining theories of product liability).

claims that personal injury, death, or property damage was caused by a manufacturing defect, design defect, or failure to warn of a known danger.[119] Courts have yet to extend product liability to defective software.[120] Product liability may fill the breach where warranty provisions in license agreements fail.[121] Courts have not considered the extension of strict liability to defective computer hardware or software, although the potential liability is great.[122]

A small number of forward-looking courts have extended product liability concepts to information products. One California court, for example, imposed liability on the seller of an inaccurate instrument approach chart.[123] Most courts tacitly assume that a dissatisfied software licensee has recourse under Article 2 of the UCC, but the universal disclaiming of warranties and remedies deprives users of any real protection. No court has yet applied the *Restatement (Third) of Torts: Product Liability*, adopted by the American Law Institute in 1997, in a defective software case.[124] Given the *Restatement (Third's)* retreat from strict liability to a negligence-based standard, it seems unlikely that the courts adopting the *Restatement* will be receptive to stretching product liability concepts to software, digital information, and other intangibles.[125] A defective soft-

119. Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 88-93 (2002).

120. *See* Patrick T. Miyaki, Comment, *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) (arguing that a computer software manufacturer should not be held liable for defective software under strict product liability); Michael R. Maule, Comment, *Applying Strict Product Liability to Computer Software*, 27 TULSA L.J. 735, 756 (1992).

121. Peter Alces, *W(h)ither Warranty: The B(l)oom of Product Liability Theory in Cases of Deficient Software Design*, 87 CALIF. L. REV. 269 (1999) (explaining how strict liability could fill the void caused by the failure of warranty in license agreements).

122. *Lessons to Learn Regarding Restatement Product Liability*, 15 COMP. LAW STRAT. 5 (Oct. 1998).

123. Fluor Corp. v. Jeppesen & Co., 170 Cal. App. 3d 468, 476 (Ct. App. 1985) ("[A] sheet of paper might not be dangerous, per se, it would be difficult indeed to conceive of a salable commodity with more inherent lethal potential than an aid to aircraft navigation that, contrary to its own design standards, fails to list the highest land mass immediately surrounding a landing site"); *see also* Saloomey v. Jeppesen & Co., 707 F.2d 671 (2d Cir. 1983) (applying Colorado law); Brocklesby v. United States, 767 F.2d 1288, 1298 (9th Cir. 1985).

124. RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 19 cmt. a (1998).

125. *See id.* On the warranty side, courts have been more willing to expand Article 2 concepts even though software is an intangible. *See generally* Amy H. Boss & William J. Woodward, *Scope of the Uniform Commercial Code; Survey of Computer Contracting*

ware case could be tried on grounds of a manufacturing defect, a failure to warn or a design defect. Courts are currently evaluating such a theory; in the Microsoft class action, the plaintiff argued that the software vendor's warnings were inadequate.[126]

A "risk-benefit" test should be utilized to ascertain whether public policy supports holding the software industry liable for defective software.[127] Software vendors argue that the "benefit" of reduction in risk does not justify the burden of extending product liability to defective software.[128] We believe, in contrast, that the "magnitude of the risk" is so great that increased incentives are necessary to motivate companies to produce safer products and services.[129]

Courts have had little difficulty extending product liability for bad software when the design defect causes physical injury or death.[130] Catastrophic software failure has been the cause in fact of major accidents in a variety of fields.[131] Software failure, for example, was the probable cause of the crash of a Boeing 757 that killed seventy people in Peru.[132] A New Jersey court applied product liability law in a case in which the brakes of a tractor-trailer failed because of defective software on the vehicle's onboard computer.[133] The plaintiff's product liability case was based on the

---

Cases, 43 BUS. LAW. 1513 (1988); Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply*, 35 EMORY L.J. 853 (1986); Bonna Llyn 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).

126. *See* Lohr, *supra* note 23 (documenting industry's determined opposition to product liability theories being extended to software).

127. In defective software cases, the factors most relevant to liability are awareness or constructive knowledge of high-level risks balanced against the burden of eliminating the vulnerabilities. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 3 (Proposed Final Draft No. 1, Apr. 6, 2005).

128. *See* Lohr, *supra* note 23.

129. *Id.*

130. *See generally* Miyaki, *supra* note 120, at 121.

131. Diane Savage, *Avoiding Tort Claims for Defective Hardware and Software Strategies for Dealing with Potential Liability Woes*, 15 COMP. LAW STRAT. 1 (1998).

132. *Computer Failure Puzzling in Peruvian Crash* (CNN television broadcast Oct. 3, 1996); *see also Computer Failure Puzzling in Peruvian Crash*, CNN.COM, Oct. 3, 1996, http://www.CNN.com/world/9610/03/peru.crash.

133. Roberts v. Rich Foods, Inc., 654 A.2d 1365, 1367, 1372-73 (N.J. 1995) (describing the issue of whether defective computer software caused a truck accident). In *Roberts*, the court remanded the case for a new trial in light of its interpretation of a defense to the New Jersey Product Liability Act of 1987 (NJPLA). The court ruled that the trial court must require the plaintiff to prove that the manufacturer could have eliminated the software defect or "danger without eliminating an inherent characteristic of the product, and thereby significantly diminishing the product's intended use." *Id.* at 1373.

claim that the "on-board computer used to record a truck's toll and mileage information was defectively designed to be operated by the driver while the truck was in motion and that this resulted in" the collision.[134] A jury decided that the on-board computer was not defective, but the New Jersey Supreme Court reversed, finding that the jury had been improperly instructed.[135]

The Alabama Supreme Court considered a case in which a driver's grandson was killed when his Chevrolet pickup truck stalled in an intersection and was struck by a logging truck.[136] A defective computer chip that controlled engine functions, including the fuel delivery system, contributed to the accident.[137] The jury awarded $15 million in punitive damages based upon evidence that General Motors knew about the stalling problems in their vehicles but took no prompt remedial action to protect the consuming public.[138]

Although product liability concepts have been extended to durable goods that incorporate software, they have never been applied defective software alone[139] because such causes of action were initially conceived as remedies for personal injury, rather than for financial loss.[140] In most cases, an empirically-based risk/benefit calculation is impossible because information concerning the foreseeable likelihood of a computer intrusion and the burden of risk-prevention measures is limited. However, it makes little sense to hold a manufacturer liable for software failure when the programming code is embedded in a tangible product but not where the software is a stand-alone product. As software displaces the durable goods-based economy, it is critical to develop remedies with teeth in order to make the industry more accountable.[141]

---

134. *Id.* at 1368.

135. *Id.* at 1374 (remanding the case to trial court).

136. General Motors Corp. v. Johnston, 592 So.2d 1054 (Ala. 1992).

137. *Id*. at 1056.

138. *Id.* at 1057.

139. Some commentators have urged extending strict product liability principles to software. *See, e.g.*, Lori A. Weber, *Bad Bytes: The Application of Strict Product Liability to Computer Software*, 66 ST. JOHN'S L. REV. 469 (1992); Miyaki, *supra* note 120, at 121. To date, no court has accepted the invitation to apply strict liability to computer software defects.

140. *See, e.g.*, Suter v. San Angelo Foundry & Mach. Co., 406 A.2d 140, 151-52 (N.J. 1979) (discussing Judge Guido Calabresi's efficiency-based argument for strict product liability).

141. IBM introduced the concept of the PC, or personal computer, in a 1981 press conference. By 1990, the software industry's revenues were growing many times faster than revenues for computer hardware. Rustad, *supra* note 45, at 566.

Another obstacle to imposing product liability for defective software is the economic loss rule that precludes recovery in tort where the injury is pecuniary and there is no claim for physical injury, death, or other property damages.[142] The economic loss rule foiled the plaintiffs in *Benning v. Wit Capital Group, Inc.*,[143] where the customers of an internet brokerage firm alleged that the company "owed a duty of reasonable care to maintain the facilities and support systems necessary to provide the services offered its members."[144] In *Benning*, the plaintiffs argued that the online brokerage house "failed to use reasonable care in managing customer orders in a fair, consistent, and reasonable manner as required by professional governing standards."[145] The court dismissed the claims of fraud and negligent misrepresentation because, under Delaware law, purely economic losses are not recoverable by way of a tort claim.[146] Similarly, in *NMP Corp. v. Parametric Tech. Corp.*,[147] an Oklahoma court held that the economic loss doctrine barred negligence claims for defective software. Courts have largely been unreceptive to stretching strict product liability to purely economic losses such as damage to hard drives caused by destructive computer viruses. Courts may be more willing to recognize a negligent enablement theory of product liability where prior similar computer intrusions signal a software manufacturer's ill-considered design decisions.

---

142. The end-user's right to seek recovery from the manufacturer . . . of a product . . . when the user does not directly deal with the manufacturer . . . often hinges on product liability concepts. In most states, however, product liability claims are not available for pure economic loss. . . . In cases of economic loss, the primary avenue of recovery must flow through contract law theory.

Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103, 107 (Tex. 2002) (citation omitted); *see also* East River Steamship Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 871 (1986) (stating that the economic loss doctrine limits damages "[w]hen a product injures only itself"); Apollo Group v. Avnet, 58 F.2d 477, 479 (9th Cir. 1995) (stating that the economic loss rule bars recovery in tort where the injury is only pecuniary); Southwestern Bell Tel. Co. v. Delanney, 809 S.W.2d 493, 491 (Tex. 1991).

143. No. 99C-06-157, 2001 Del. Super. LEXIS 7, at *1 (Del. Super. Ct. Jan. 10, 2001).

144. *Id.* at *19-20.

145. *Id.*

146. *Id.* at *21.

147. 958 F. Supp. 1536, 1546-47 (N.D. Okla. 1997) (rejecting negligence claim for defective software because of economic loss rule).

2. Licensing of Tangibles, Not Sales of Goods

The concept of the breach of an implied warranty of merchantability, like strict liability, does not turn on fault.[148] Courts are inclined to classify software as goods—especially if the programming code is incorporated in a computer system—but there are problems with this approach.[149] Software is neither a good nor a product, but rather an intangible collection of digital information: code composed of 1s and 0s. Software licenses permit licensees to use information, but do not transfer title. Software is licensed with restrictions on the conditions of use and is therefore unlike tangible products that can be used at the discretion of the purchaser. Network security software is frequently a hybrid of sales and services. The mixed character of software creates the legal dilemma of whether to treat it as the sale of goods under Article 2 of the UCC, or as the rendering of professional services.

3. Premises Liability for Computer Software

Protecting computer users from third-party cybercrime parallels concepts of premises liability.[150] Marketing software with a known security defect is analogous to not having a front door on an apartment building. In

148. In order to prevail in an Article 2 implied warranty of merchantability lawsuit, a plaintiff need only prove that the delivered goods failed to be at least fair average quality, did not run within variations specified in the contract, were inadequately contained or packaged, or deviated from one of the six measures of merchantability found in U.C.C. § 2-314 (2005). To be merchantable, goods must satisfy each of the following standards: (1) pass without objection in the trade; (2) be of fair, average quality; (3) be fit for the ordinary purpose of the product; (4) have evenness of quality; (5) be adequately contained; and (6) conform to the representations on the label. U.C.C. § 2-314(2). U.C.C. § 2-314 has no requirement that the dissatisfied buyer prove fault of the seller; just as in product liability, the entire focus is on the delivered goods rather than what the seller did or did not do.

149. Courts frequently extend Article 2 to software where the predominant purpose of the computer contract is a sale rather than a service. Article 2 supports this broad reading of Article 2's scope which uses the phrase "transactions in goods," including "specially manufactured goods." U.C.C. § 2-102. It is arguable that "transactions in goods" includes software in a transaction that also includes hardware. *See* Colonial Life Ins. Co. v. Elec. Data Sys. Corp., 817 F. Supp. 235 (D.N.H. 1993) (extending Article 2 to software in a mixed transaction); *see also* Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670 (3d Cir. 1991); RRX Indus., Inc. v. Lab-Con, Inc., 772 F.2d 543 (9th Cir. 1985); Sys. Design v. Kansas City Post Office, 788 P.2d 878 (Kan. Ct. App. 1990).

150. In a premises liability case against a landowner, it is critical to establish that a landowner owed the plaintiff a duty of care. As a general rule, a landowner must exercise ordinary care to avoid reasonably foreseeable risks of injury to the entrant on the land. *See* Crowley v. Westside City, No. E033634, 2004 Cal. App. LEXIS 670 (Ct. App. Jan. 26, 2004).

premises liability, a property owner who invites the public onto his property for business purposes is potentially liable if those invitees are harmed by negligent or accidental attacks by third parties.[151]

To prevail in a premises liability lawsuit, a plaintiff must establish that: (1) the defendant owed a duty to protect the injured crime victim; (2) the defendant breached that duty; and (3) the breach of the duty was a proximate cause of the criminal act and the victim's injuries.[152] Premises liability lawsuits are brought against the owners of residential property, hospitals, colleges, day care centers, and shopping centers whose inadequate security enables criminals who attack customers.[153] The duty of reasonable computer security will require a similar analysis and useful analogies may be drawn from contract, public duties, statutes, or ordinances. Courts have extended the concept of premises liability for inadequate security to shopping malls, parking lots, and apartment complexes but never to software or networked computer systems.

The seller of inadequately configured software may expose its customers to predators just like a retail establishment that fails to employ security guards in a high crime area.[154] A software vendor may owe a duty of care to its customers as well as to third parties that makes it liable for enabling the conversion of credit card numbers, the invasion of privacy, identity theft, or the misappropriation of trade secrets. Courts may find such a vendor liable for rushing poorly tested software to market.[155] In such a situation, a computer vendor may avoid liability by building in comprehensive security solutions that reduce the cybercrime rate.

Concepts developed for landowner or occupier liability do not fit well with the ethereal nature of cyberspace. The law of premises liability de-

---

151. The comment to Section 432 of the *Restatement (Second) of Torts* states that subsection (1) applies "where the actor's tortious conduct consists in a failure to take some precautions which are required for the protection of another's person or land or chattels." RESTATEMENT (SECOND) OF TORTS § 432 cmt. b (1979).

152. ALAN KAMINSKY, A COMPLETE GUIDE TO PREMISES SECURITY LITIGATION 7 (2d ed. 2001).

153. *Id.* at 5.

154. Premises liability is based on the notion of prior similar acts that establish the foreseeability of harm. *See, e.g.*, K.L. v. Riverside Medical Ctr., 524 N.W.2d 300 (Minn. Ct. App. 1994).

155. There is no case law on whether an implied contract to provide a secure environment applies to cyberspace. In K.M.H. v. Lutheran Gen. Hosp., 431 N.W.2d 606, 608 (Neb. 1988), the Nebraska Supreme Court held that the hospital entered into an implied contract to provide patients with a secure environment. In that case, a male employee performing a bed check sexually assaulted a patient. *Id.* at 607. A hospital seemingly would owe a higher duty to vulnerable patients than an online business would owe to its customers.

termines the degree of a landowner's liability based upon the status of the entrant: (1) trespasser;[156] (2) licensee;[157] and (3) invitee.[158] In the bricks and mortar world, the possessor of land owes duties, in descending order, to invitees, licensees, and trespassers. To be liable to business invitees, the land possessor must discover that crimes are being committed and then fail to give a warning that is adequate "to enable the visitors to avoid the harm, or otherwise to protect them against it."[159]

The most significant doctrinal obstacle to extending premises liability to the internet is that cyberspace is borderless and does not involve land, which makes all landowner classifications problematic. In the law of premises liability, courts have constructed a number of tests to determine when a defendant should be liable for enabling the crimes of third parties. The "specific harm" case in premises liability holds landowners liable for failing to protect patrons from the violent acts of third parties once they become aware of specific imminent harms.[160] If this approach were adopted for computer software cases, the vendor's duty of care would be triggered only if the vendor knew of a specific cybercrime threat and failed to redesign the software to respond to that risk. This narrow approach would mean that few, if any, software vendors would be liable because prior knowledge of a cybercrime threat from a specific individual is unlikely. Even if this test could be broadened, it would be unlikely that a vendor would learn of specific cyberthreats in time to avert the danger.

Courts in computer security cases will seek to avoid imposing unlimited liability. To this end, courts may require plaintiffs to prove that the computer intermediary was on notice because of a prior similar computer intrusion.[161] Under this approach, plaintiffs would prove the foreseeability

---

156. THE RESTATEMENT (SECOND) OF TORTS § 329 (1965) defines a trespasser as "a person who enters or remains upon land in the possession of another without a privilege to do so created by the possessor's consent or otherwise."

157. Traditionally, licensees, defined as social guests and others with the permission to enter the land, were owed an intermediate standard of care. *Id.* § 313.

158. The concept of the business invitee was originally developed to protect passengers on common carriers or other public utilities. *Id.* § 344. The duty to business invitees arises when the "land [is] open to the public for entry for his business purposes, and then only to those who come upon the land for the purposes for which it is thus held open to the public. Such persons are commonly called business visitors." *Id.* § 344 cmt. a.

159. *Id.*

160. *See* Posecai v. Wal-Mart Stores, Inc., 752 So. 2d 762 (La. 1999) (discussing the theory of specific harm for third party criminal acts).

161. "Foreseeability is endless because foreseeability, like light, travels indefinitely in a vacuum." Newton v. Kaiser Found. Hosp., 184 Cal. App. 3d 386, 391 (1986). In landowner owner cases, some courts have adopted a prior similar incidents test to demonstrate foreseeability. *Posecai*, 752 So. 2d at 767.

of cybercrime by presenting evidence of prior security breaches, intrusions, or virus incidents. Courts would have the most flexibility in choosing either a "totality of the circumstances" or a "balancing" test to determine whether the software vendor breached its duty.[162] A court using either of these approaches would look at all relevant circumstances including the number, nature, and location of prior similar computer crimes and the closeness of the connection between defective software and the intrusions.

Thirty-five years ago, a federal appellate court in *Kline v. 1500 Mass Ave. Apartment Corp.*[163] became the first judicial body to recognize that a landlord had a duty to protect tenants in the common area of an apartment building from foreseeable criminal attacks. The *Kline* court cited several reasons for judicial reluctance to recognize the landlord's duty to prevent third-party crimes. The policy reasons included:

> [J]udicial reluctance to tamper with the traditional common law concept of the landlord tenant relationship; the notion that the act of a third person in committing an intentional tort or crime is a superseding cause of the harm to another resulting . . . [in] the oftentimes difficult problem of determining foreseeability of criminal acts; the vagueness of the standard which the landlord must meet; the economic consequences of the imposition of the duty; and conflict with the public policy allocating the duty of protecting citizens from criminal acts to the government rather than the private sector.[164]

Similar considerations have made contemporary judges reluctant to impose a duty of care on software vendors to reduce cybercrimes.

Kline's creation of a landlord's duty to minimize risk to tenants may serve as a model for expanding liability to encompass defective software. Courts can balance the foreseeability of harm and the gravity of harm against the burden on the software industry in crafting the duty of care. Internet security is critical to the information industry but imposing too much of a burden of precaution may have a chilling effect on the information-based economy.[165] Courts should have little difficulty in supporting a

---

162. *Id.* (describing these approaches).

163. 439 F.2d 477, 483 (D.C. Cir. 1970).

164. *Id.*

165. The changing economy is illustrated by the projected increase in demand for computer software engineers, which is a professional category that is likely to develop faster than other occupations. U.S. Department of Labor, Bureau of Labor Statistics, Computer Software Engineers, http://www.bls.gov/oco/ocos267.htm (last visited Mar. 29, 2005).

generalized duty to implement virus-protection, improved software design, and industry-standard network security, but the exact limits of the duty will be difficult to determine.

The owner of a website, like any other retail establishment, could theoretically be liable for the reasonably foreseeable harm caused by third parties that injure customers. A court adopting either of these approaches should look first at the role defective design of software plays in enabling computer intrusions along with all other relevant circumstances including the number, nature, location, and response to prior security.[166] Courts should examine factors such as: (1) whether there have been prior similar cybercrimes; (2) the cost of increased internet security measures; and (3) the degree to which intermediaries can reduce the radius of the cybercrime problem. In the absence of a history of similar intrusions and security breaches, foreseeability is based on all facts and circumstances.[167]

Part IV of this Article will explore the parameters of our proposed tort of negligent enablement of cybercrime. The duties owed to a plaintiff by an online company may be based upon private duties, such as contract, or public duties, based on a statute or an ordinance. A duty of care may also arise from a vendor's failure to anticipate foreseeable tortious or criminal acts of others. A vendor, for example, could potentially be held liable for negligently permitting a third party to hack into its computer network and steal data or proprietary information owned by others, where that inadequate security results in injuries to third parties. Courts must determine whether software liability should be permitted as a matter of duty and, if so, how to balance the public interest in encouraging a dynamic software industry with the need to counter the massive harms caused by cybercriminals.

---

166. The trend in the law is to impose premises liability for injuries caused by the criminal acts of third parties. Courts have imposed a duty to maintain a secure environment against a wide array of property owners including landowners, landlords, business owners, and other possessors of land. *See generally* Shelley Ross Saxer, *Am I My Brother's Keeper? Requiring Landowner Disclosure of the Presence of Sex Offenders and Other Criminal Activity*, 80 NEB. L. REV. 522, 524 (2001) (summarizing expansion of premises liability for third-party crimes).

167. *See* Hamilton v. ACCU-TEK, 62 F. Supp. 2d 802, 818 (E.D.N.Y. 1999) ("In the usual run of cases, a general duty to avoid negligence is assumed, and there is no need for the court to undertake detailed analysis of precedent and policy." (citing RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM, Basic Principles § 6 (Discussion Draft, Apr. 5, 1999) and finding that no duty is rare); *see* Rabin, *supra* note 67, at 480 (quoting RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM, Basic Principles § 6).

IV. THE TORT OF NEGLIGENT ENABLEMENT OF CYBERCRIME

This Part examines the prima facie case for negligent enablement of cybercrime. A claim of negligent enablement requires proof of the following elements: (1) a duty of care owed by the software vendor to its customer; (2) conduct below the applicable standard of care that amounts to a breach of that duty; (3) an injury or loss; (4) cause in fact; and (5) proximate or legal cause.[168] Once the software publisher owes the licensee a legal obligation to conform to a reasonable standard of conduct, the question is whether the duty has been breached.[169] Software vendors are the "cheapest cost avoider" because they have superior information about known or developing vulnerabilities in their products or services.[170] This Part concludes by briefly discussing defenses and immunities to the imposition of liability for negligent enablement of cybercrimes.

A. Crafting a Duty of Care

The recognition of new tort duties is inevitably a policy-based determination. The judiciary will balance such factors as the foreseeability of the harm of computer viruses or other breaches of security; the degree of certainty between software vulnerabilities and harm; the connection between lax internet security practices and the injury suffered by a computer user; the policy of preventing future intrusions; the burden on the information industry and the consequences to the community of imposing a duty to maintain adequate security; and the availability, costs, and prevalence of security solutions and insurance.[171] In most instances, the software vendor creates the risk while also benefiting from the information-based economy. The judiciary should be open to crafting creative new duties of care for the information age when the magnitude of risk caused by bad software outweighs the burden of precaution.

---

168. *See*, *e.g.*, McCall v. Wilder, 913 S.W.3d 150 (Tenn. 1995) (explaining elements of negligence).

169. The more modern theory of breach is based upon risk-utility. *See* Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1054, 1060 (1972) ("The question for the court reduces to a search for the cheapest cost avoider."); *Id*. at 1060 n.19 ("The cheapest cost avoider has been . . . defined as the party an arbitrary initial bearer of accident costs would (in the absence of transaction and information costs) find it most worthwhile to 'bribe' in order to obtain that modification of behavior which would lessen accident costs most.").

170. *See generally* GUIDO CALABRESI, THE COST OF ACCIDENTS 244-45 (1970).

171. These factors are drawn from Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968).

A court's willingness to recognize a software licensor's duty of care to produce secure software is a policy-based decision tied to the radius of the risk. The common law imposes no obligation to prevent crime or even to control the actions of others.[172] However, the epidemic of software vulnerabilities constitutes a compelling reason to recognize a new duty of reasonable internet security.

Any duty to protect computer users from the cybercrimes of third persons must be predicated on a preventable risk. In many computer security cases, there may be multiple defendants who owe third party consumers a duty of care. The scope of liability will ultimately rest with the courts and be decided on grounds of duty or proximate cause. For example, where the loss is primarily economic, the courts may be reluctant to extend the duty of maintaining adequate computer security to credit card issuers. Courts are also likely to be unreceptive to claims that an issuing bank engaged in negligent marketing and distribution of insecure credit instruments.[173]

B. Determining Breach in Negligent Enablement Cases

1. Custom and Software Industry Standards

A software vendor's compliance with the customary best practices of others in the industry is strong probative evidence that the company was not negligent, but does not preclude a finding of negligence where the industry's standards are lax.[174] In the software industry, the failure of a licensor to incorporate a risk-reducing precaution adopted by others in the community should be given significant weight.[175] In traditional tort law, courts frequently turn to industry standards or custom to determine best

---

172. JOHN DIAMOND, UNDERSTANDING TORTS 133 (1999) ("As a general principle, there is no obligation to protect another from harm.").

173. Courts have not been receptive to finding for the victims of physical injury under a negligent marketing and distribution theory, so it is even more unlikely that the duty will be extended in economic loss cases. *See generally* Hamilton v. Beretta U.S.A. Corp., 750 N.E.2d 1055 (N.Y. 2001) (holding that the manufacturers of hand guns owed no duty on grounds of negligent marketing under diverse theories such as market share or alternative liability).

174. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 13 (Proposed Final Draft No. 1, Apr. 6, 2005) (describing the powerful role of customs as the source of legal obligations and in tort law as the test of "ordinary care").

175. *Id.* § 13 cmt. c (noting that "the actor's departure from custom—its failure for example to incorporate a risk-reducing precaution adopted by others in the same line of activity—tends to answer relevant questions concerning the availability and feasibility of appropriate precautions").

practices in a given field.[176] Private standards such as best practices or industry safety codes may be used in bad software litigation to establish negligence by departure from custom.

In the field of financial services, for example, the industry has developed the Payment Card Industry (PCI) Data Security Standard that went into effect on June 30, 2005.[177] The PCI standard requires all retailers, online merchants, data processors, and other businesses that handle credit card information to encrypt data, incorporate end-user access control, and devise activity monitoring and logging systems.[178] This financial industry standard also mandates "formal security policies and vulnerability management programs."[179] A software company's departure from this standard provides some evidence of negligence.[180] Proof that a software vendor has failed to incorporate industry-wide precautions in its design or testing of a new product or service will help the fact finder determine whether the company has acted with ordinary care.

Custom provides the floor, but not necessarily the ceiling, of reasonable care. A threshold question for setting the standard of care for software design is to examine whether compliance to industry standards should be a complete defense against a negligence claim.[181] Software companies should be required to constantly update and adapt their security protocol. Vendors designing UNIX systems, for example, should have a duty to reasonably minimize security holes. Yet, at present, "Unix systems, with their large number of built-in servers, services, scripting languages, and inter-

176. *See generally* Richard A. Epstein, *The Path to the T.J. Hooper: The Theory and History of Custom in the Law of Tort*, 21 J. LEGAL STUD. 1 (1992).

177. Jaikumar Vijayan & Todd Weiss, *CardSystems Breach Renews Focus on Data Security A New Data Protection Standard Goes Into Effect Next Week*, COMPUTERWORLD, June 20, 2005, http://computerworld.com/securitytopics/security/story/0,10801,102646,00.html.

178. *Id.*

179. *Id.*

180. *See, e.g.*, Trimarco v. Klein, 436 N.E.2d 502, 506-07 (N.Y. 1982) (discussing the probative value of deviation from custom as evidence of negligence).

181. Companies should institute and enforce stringent computer security policies, provide organizational training and awareness of computer security issues and conduct regular security audits to ferret out security weaknesses. Companies should also implement and, to the extent feasible, require their vendors to implement the latest security technologies such as firewalls, anti-virus software, intrusion detection systems, and encryption of its most sensitive data. Finally, a company should investigate obtaining insurance coverage for computer security liability. Many general commercial liability policies exclude coverage for computer-related liability. Bradford D. Bimson, *Poor Tech Security Can Mean Lawsuits*, THE VIRGINIAN-PILOT, Nov. 16, 2003, http://www.williamsmullen.com/news/articles_detail/122.htm.

preters, are particularly vulnerable to attack because there are simply so many portals of entry for hackers to exploit."[182] A vendor's compliance with lax security protocols should not shield it from negligent security claims.

In *The T.J. Hooper*,[183] Judge Learned Hand found an industry custom of not having radios aboard barges to be negligence even though this precaution was not widely adopted. Judge Hand rejected the barge owners' argument that they were not negligent because the industry had not yet generally adopted receiving sets, stating "a whole calling may have unduly lagged in the adoption of new and available devices."[184] The *T.J. Hooper* decision stands for the proposition that compliance with custom is not an absolute defense to negligence. Just because a software vendor complies with inadequate testing standards does not immunize the company from a finding of negligence. Businesses that use wireless computer networks may be found to be negligent because of unacceptable risk even though many companies fail to use adequate security.[185] Custom is a good test for reasonable care only when industry practices do not create unreasonable preventable dangers.[186]

Since private industry standards are relatively undeveloped for the software industry, custom is less important in setting the standard of care in the software industry. It may be premature to turn to industry standards in many areas where there is no consensus as to custom or standard.[187] An actor's compliance with industry standards will be a good test for negligence once best practices are established. Independent laboratories now have devised protocols for testing computer networks for their vulnerability to intrusions.[188] Certifying organizations must develop standards for properly configuring voice, video, fax, and data traffic between conventional telephone networks and packet-based data networks such as the internet. Partnerships between government and industry may be helpful in

182. W3C World Wide Web Security FAQs, http://www.w3.org/Security/faq/wwwsf1.html#GEN-Q3 (last visited Mar. 5, 2004).

183. 60 F.2d 737 (2d Cir. 1932).

184. *Id.* at 740.

185. Drew Clark, *Cyber Security: White House Aide Criticizes Progress Toward Internet Security*, NAT'L J.'S TECH. DAILY, July 30, 2002.

186. *See generally* Epstein, *supra* note 176.

187. *See* Robin A. Brooks, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343, 360 (1998).

188. Press Release, TruSecure, ICSA Labs Certifies Network Intrusion Detection Systems in Phase One of Testing in Multiple Network Environments (July 29, 2002), *available at* http://www.trusecure.com/company/press/release618.shtml.

certifying industry standards.[189] Compliance with internet industry standards should be interpreted as some evidence of compliance with due care, rather than a complete defense against negligence-enabling claims.[190]

2. Computer Malpractice

The common law imposes a higher duty of care upon professionals such as doctors or lawyers.[191] In the field of medical malpractice, courts determine whether physicians exercised the care and skill of the average qualified practitioner.[192] In the future, it is possible that courts will hold internet security professionals to a higher professional standard of care, similar to those currently imposed on doctors, lawyers, accountants, and other established professionals.[193] Computer security may become professionalized with credentialing and accreditation procedures. Certification in the future may focus on specialized training in examining binary data for malicious code, creating the architecture for safe corporate computer security, and identifying software vulnerabilities.[194]

It is theoretically possible that a software engineer could be held liable for computer malpractice but, to date, no court has held that a software engineer's failure to develop reasonably secure software constituted professional negligence. The field of computer security is just beginning to mature, making it difficult for courts to determine professional standards

189. There is no case law or commentary on the question of whether the government would be liable for negligent security under the Federal Tort Claims Act for harm caused by negligent information security. The discretionary function exception may be extended to immunize the government against claims for negligent security where there are rapidly evolving standards of information security. *See* William P. Kratzke, *The Supreme Court's Recent Overhaul of the Discretionary Function Exception to the Federal Tort Claims Act*, 7 ADMIN. L.J. AM. U. 1 (1993) (discussing how courts would apply the discretionary function to a wide range of governmental activities).

190. Rustad & Eisenschmidt, *supra* note 4, at 248 (arguing that failure to comply with industry security standards constitutes negligence).

191. *See* RESTATEMENT (SECOND) TORTS § 299A (1965).

192. Brune v. Belinkoff, 235 N.E.2d 793 (Mass. 1968).

193. *See* Steiner Corp. v. Johnson & Higgins of Cal., 135 F.3d 684, 688 (10th Cir. 1998) (holding that a professional who held himself out as a professional was liable for the negligent performance of duties undertaken); *In re* Daisy Sys. Corp., 97 F.3d 1171, 1175 (9th Cir. 1996) (holding that a duty of professional care required the plaintiff to show that the defendant should have used such skill, prudence, and diligence as other members of his or her profession commonly possessed and exercised); *see also* Hosp. Computer Sys., Inc. v. The Staten Island Hosp., 788 F. Supp. 1351, 1361 (D.N.J. 1992); Heath v. Swift Wings, Inc., 252 S.E.2d 526, 529 (N.C. App. 1979).

194. *See generally* Sandra Lancaster & Oneil Cross, *Security Academic Programs*, 1 J. SECURITY EDUC. 131 (2005) (classifying and describing academic programs specializing in computer security).

of care.[195] No court has held a software company liable for failing to meet professional computer security standards. Courts have also been reluctant to recognize the tort of computer malpractice for negligent design of hardware or software.[196]

Software engineering is a relatively new field without the well-established professional standards that are found in more developed professions such as law and medicine. For example, medical specialists must pass far more stringent board certifications than the optional certification examinations provided by various computer services vendors. Courts have uniformly rejected attempts to apply a professional standard of care to software engineers, designers, or consultants despite the fact that software designers and computer engineers have professional organizations that set standards.[197] In *Heidtman Steel Products v. Compuware Corp.*,[198] the Ohio federal court refused to extend the concept of professional malpractice to a negligent computer consultant under Michigan law.[199] Courts will not apply the professional standard of care to software engineers and other professionals until they can reliably assess the skill and expertise required of software engineers.

---

195. One organization establishing standards is the International Information Systems Security Certification Consortium, or $(ISC)^2$, which promotes the Certification for Information System Security Professional (CISSP) certification exam to aid in the evaluation of personnel performing information security functions. Welcome to CISSP.com, http://cissp.com/ (last visited Dec. 10, 2005).

196. While early cases found that software vendors owed no professional duty of care, one court found this was a question for the jury to decide. Savage, *supra* note 131 (discussing Diversified Graphics v. Groves, 868 F.2d 293 (8th Cir. 1989)).

197. The IEEE Computer Society and ACM have established standards for their members. The Institute for Certification of Computing Professionals has an ethics code for its certified members. If a developer is a member of IEEE, the developer accepts their code of performance. The IEEE is a society for engineers (traditional professionals), and therefore software developers could be held to a similar level of liability as their professional counterparts. Even if software development cannot be declared a profession, a member of a skilled trade can also be held to the standards of care and practice for that trade. If programmers are not judged professionals, they are certainly practitioners of a skilled trade. Karen Hooten, *'Twas the Day after Christmas: Legal Issues Facing Software Developers: Programming by Profession*, 9 COMPUTER LANGUAGE 105 (1992); *see* Patricia DiRuggiero, *The Professionalism of Computer Practitioners: A Case for Certification*, 25 SUFFOLK U. L. REV. 1139 (1991) (arguing for the extension of the professional standard of care to computer specialists).

198. No. 3-97CV7389, 1999 U.S. Dist. LEXIS 21700, at *1 (N.D. Ohio, Feb. 15, 1999).

199. *Id.* at *34-*35.

3. Statutory Violations as Negligence Per Se

A statute that declares certain conduct or practices to be unlawful may also serve as a measure of whether a software vendor is liable for negligence per se in its marketing of products or services. Legislatures, however, have been slow to enact critically needed statutory standards and administrative regulations governing computer security.[200] At present, no federal or state statutory standard that plaintiffs might use as a proxy for the standard of care governs software quality. However, the violation of such a statute could establish breach of a common law standard of care.[201]

Although courts vary in what impact a statutory violation has on the adjudication of negligence,[202] they may employ civil statutes to set standards in negligent enablement lawsuits.[203] An unexcused violation of a

---

200. However, the computer security requirements of the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and the Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 501-527, 113 Stat. 1338, 1436-50 (1999), may be useful in a defective software case.

HIPAA applies to the privacy of medical records and protects all "individually identifiable health information" held or transmitted by a covered entity. 45 C.F.R. § 160.103 (2004). HIPAA's privacy rule prohibits covered entities from using or disclosing individually-identifiable information unless authorized by the statute. *Id.* § 164.502(a). The Department of Health and Human Services, which issues privacy and security regulations regarding personal data, has also released rules that require covered entities to safeguard information. *See id.* §164.530(c)(1).

The GLBA creates an affirmative obligation on the part of financial institutions to prevent the disclosure of personal information. 15 U.S.C. § 6802 (2000). The GLBA safeguarding provision requires financial institutions to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards-- (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." *Id.* § 6801(b).

201. *See* Stewart Baker & Maury Shenk, *A Patch in Time Saves Nine: Liability Risks for Unpatched Software*, 18 CORPORATE COUNSELOR 1 (Apr. 2005) (noting that although "neither HIPAA nor GLBA provides private individuals with a right to sue, these statutes could have significant weight in private actions under common law").

202. *See* RUSSELL L. WEAVER ET AL., TORTS: CASES, PROBLEMS & EXERCISES 163 (2d ed. 2004).

203. The court may adopt the standard of conduct defined by legislation or regulation where there is a:

> legislative enactment or an administrative regulation whose purpose is found to be exclusively or in part:
> (a) to protect a class of persons which includes the one whose interest is invaded, and
> (b) to protect the particular interest which is invaded, and

statute requiring reasonable security is itself negligence, that is, negligence per se.[204] Three factors are used for determining the propriety of adopting a statute as the standard of care: (1) Does the statute provide specific guidance on the standard of care? (2) Was the statute enacted to protect against the harm suffered by the plaintiff? and (3) Was the plaintiff included in the class protected by a statute?[205]

Since the internet is fairly new, there is little by way of legislative guidance on what constitutes reasonable security. No legislative body has articulated specific rules or even a general level of care applicable to all internet security cases. If statutes were enacted specifying a given level of computer security, users could use the violation of that statutory standard of care as a potent surrogate for negligence.[206] Conversely, software vendors could defend against claims of defective software by arguing that it complies with the statutory requirements.[207] In the automobile industry, manufacturers must comply with National Highway Traffic Safety Administration (NHTSA) standards.[208] It is unclear why Firestone is account-

---

> (c) to protect the interest against the kind of harm which has resulted, and
>
> (d) to protect the interest against the particular hazard from which the harm results.

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

204. A plaintiff must prove four elements in a negligence per se case. *Id.* (listing four elements). The Restatement also comments that:

> Even where a legislative enactment contains no express provision that its violation shall result in tort liability, and no implication to that effect, the court may, and in certain types of cases customarily will, adopt the requirements of the enactment as the standard of conduct necessary to avoid liability for negligence. The same is true of municipal ordinances and administrative regulations.

Id. § 285 cmt. c.

205. DIAMOND, *supra* note 172, at 95.

206. When a statute sets the standard of care, jurisdictions differ in the legal significance of a statutory violation. The majority of jurisdictions treat the breach as negligence per se, while a minority of jurisdictions considers the statutory violation as evidence for the jury to consider in determining whether there has been a breach in the standard of care. *Id.* at 98.

207. David G. Owen, *Special Defenses in Modern Product Liability Law*, 70 MO. L. REV. 1, 13-21 (2005) (discussing trends in the statutory compliance defense in product liability litigation).

208. *See* Regulations & Standards, http://www.nhtsa.dot.gov/cars/rules/ (last visited Dec. 9, 2005).

able for defective tires whereas Microsoft is immune from claims when it "produces an operating system with two systemic flaws per week."[209]

At present, federal and state regulations have not been used in any systematic way to set standards for software quality.[210] The next Section will show how federal statutes requiring reasonable levels of computer security may offer strong probative evidence for the plaintiff in bad software cases. Federal statutes not only declare conduct unlawful but specify that the violator is liable for damages to the victim of security breaches. The following statutes may be used to calibrate a standard of computer security because they declare certain conduct unlawful. If Congress has chosen to attach liability to a security breach, courts should be able to determine that conduct in violation of such a statute is unreasonable.

a) HIPAA's Security Rule

Potentially, a software licensee could use The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[211] to prove negligent enablement of a computer intrusion.[212] HIPPA prohibits a person from knowingly using a "unique health identifier" or wrongfully obtaining "identifiable health information relating to an individual" or disclosing "individually identifiable health information to another person."[213] Arguably, a provider that uses software with a known vulnerability is, in effect, knowingly disclosing private health information to unauthorized third parties such as cybercriminals. HIPPA's general privacy rule is that a "cov-

---

209. *Business: Liability Rules for Software Firms Irk Consumer Advocates*, NAT. J.'S TECH. DAILY, Sept. 12, 2003 (quoting Bruce Schneier, Computer Security Expert).

210. One problem with the preemption argument is that Congress has not expressly preempted tort actions in its internet security statutes and regulations. Another problem for the computer manufacturer is that compliance with statutory obligations does not preclude a finding of negligence.

> Courts and commentators long ago rejected the idea that an actor whose conduct comports with a safety standard required by statute or administrative regulation is automatically protected from tort liability for harm resulting from that conduct. Courts on infrequent occasions do make an exception to the general rule in limited situations where a defendant conformed its behavior precisely as directed by an especially well- considered government standard. But it is fundamental law that governmental safety standards adopt only a minimum safety floor below which an actor may face criminal sanctions but above which due care may require the actor to be more cautious.

Owen, *supra* note 207, at 14.

211. Congress addressed security and electronic signature standards and other administrative simplification issues in HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

212. *See* Bimson, *supra* note 181.

213. 42 U.S.C. § 1320d-6 (2000).

ered entity may not use or disclose protected health information, except as permitted or required."[214] A "covered entity" must "make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[215] The purpose of HIPPA's security rule is to have entities "implement[] and maintain appropriate security measures to protect that information."[216] HIPPA does not authorize a private cause of action,[217] let alone an indemnification action. The HIPPA statutory framework "expressly provides a method for enforcing its prohibition upon use or disclosure of individual's health information—the punitive imposition of fines and imprisonment for violations."[218] Health care providers punished for such unauthorized disclosers of individually identifiable health information should be able to seek indemnification against a software vendor whose products or services paved the way for the wrongful disclosure. Tort actions against the software vendor will supplement HIPPA's statutory goal of safeguarding electronic health information.

Congress enacted HIPAA to allay the increasing public concern about the threat to privacy posed by interconnected electronic information systems.[219] HIPAA regulations are designed to protect medical records from computer intruders who may misuse, misappropriate, or alter them.[220] However, to invoke a negligence per se argument based on HIPAA, the victims of defective software must establish that HIPAA was meant to encompass the foreseeable consequences of security flaws. HIPAA's internet security regulations have three purposes:

> (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of

214. 45 C.F.R. § 164.502(a) (2005).

215. *Id.* § 164.502(a)(2)(ii)(b).

216. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).

217. *See* Univ. of Colo. Hosp. Auth. v. Denver Publ'g. Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004).

218. *Id.*

219. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82465 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

220. Press Release, Dept. of Health and Human Servs., HHS Proposes Security Standards for Electronic Health Data, Aug. 11, 1998, http://www.hhs.gov/news/press/1998pres/980811.html.

> care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organization and individuals.[221]

A victim of a computer intrusion would need to prove that she was within the class of potential victims protected by the statute and was injured in the manner contemplated by the statute in order to establish negligence per se.

The software vendor will argue that the scope of its duty to secure data should be limited to standards explicitly enacted by Congress. Since Congress has enacted no private cause of action, the victims of computer intrusions have no federal civil remedy. It is even more unlikely that courts will find that Congress intended to impose liability on software vendors for enabling the theft of patients' medical records. Congress has yet to enact, or even seriously consider, any statute imposing secondary liability for computer intrusions. The statutory duty to maintain adequate computer security is on the health care provider, not the software vendor, irrespective of whether its product was marketed with known vulnerabilities. HIPAA, therefore, offers little hope to the victims of security flaws introduced by software.

b) GLBA's Information Privacy Provisions

Likewise, the victim of a computer intrusion that resulted in a breach of confidentiality of financial information will find it difficult to use a statutory violation of the Gramm-Leach-Bliley Act (GLBA) to make a negligence per se argument. When Congress enacted the GLBA in November of 1994,[222] its intent was to require financial institutions to respect the privacy of their customers and to protect the security and confidentiality of these customers' nonpublic personal information.[223] GLBA compliance requires that each financial institution secure data, including credit card information, transmitted on the internet.[224]

The GLBA prohibits financial institutions from disclosing nonpublic personal information about customers to nonaffiliated third parties unless

---

221. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

222. The Commission issued final rules governing the GLBA on May 24, 2000. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (May 24, 2004) (codified at 16 C.F.R. 313).

223. *See* 15 U.S.C. § 6801 (2004) (entitled Protection of Nonpublic Personal Information).

224. *Id.*

there are adequate disclosure. Financial institutions must provide customers with an opportunity to opt out if they object to divulging or sharing personal information.[225] In addition, the financial institution must disclose its privacy policy both at the time it enters into a fiduciary relationship with a consumer "and not less than annually during the continuation of such relationship."[226] As with HIPAA, the express statutory purpose applies to financial institutions rather than to the software developers that enabled the theft of personal data or financial information, undercutting the likelihood that the statute could be the basis of a negligence per se claim.

c) California's Security Breach Information Act

California's recently-enacted statute requiring notification of a computer security breach involving personal information seems to be the best candidate for a negligence per se claim against software publishers or vendors.[227] The Business Roundtable opposes legislation requiring companies to report computer security breaches or implement minimum security standards because these obligations may lead to greater litigation costs.[228] However, California requires all companies to report network security breaches in order to protect that state's residents against identity theft and to encourage businesses to improve their network security.[229] Any person or business maintaining computerized data that includes personal information[230] has an affirmative obligation to "notify the owner or licensee of the information of any breach of the security of the data imme-

225. *See* 15 U.S.C. § 6802(b)(1) (2005) (stating that consumer must be given an opportunity to opt out before private financial information may be disclosed to third parties).

226. 15 U.S.C. § 6803 (2004).

227. CAL. CIV. CODE § 1798.82 (2005); *see, e.g.*, Cheryl A. Falvey et al., *Disclosure of Security Breaches Required by New California Privacy Legislation*, METRO. CORP. COUNS., Aug. 2003, at 5 (stating that "many predict that the disclosure obligation will result in massive class action suits for companies victimized by security breaches"); Melissa Solomon, *Bank Allies Say California Hacking Law Goes Too Far*, 16 BANK TECH. NEWS 37 (Mar. 2003).

228. David Bank, *Companies Seek to Hold Software Makers Liable for Flaws*, WALL ST. J., Feb. 24, 2005, at B1.

229. CAL. CIV. CODE § 1798.82 (2005) (discussing disclosures of breach insecurity by businesses maintaining computerized data that includes personal information).

230. Personal information is defined as an unencrypted combination of data including a person's first name (or first initial) and last name in combination with: "(1) social security number, (2) driver's license number or California Identification Card number, or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." CAL. CIV. CODE § 1798.82(e) (2005).

diately following the discovery" of the breach if data was believed to be acquired by an "unauthorized person."[231]

A company failing to promptly notify the victim whose personal information has been intercepted on the internet is liable for statutory damages and equitable relief. In addition, a company may be vulnerable to a common law action for negligence per se.[232] The first lawsuit under California's computer security breach notification statute was filed as a class action in 2003.[233]

Although laws such as California's security breach notification statute hold some promise for negligence per se causes of action, clear statutory standards of care at either the state or federal levels have yet to be enacted that would serve as a basis for negligence per se findings in defective software lawsuits.

4. Risk/Utility Methods of Calibrating Due Care

Judge Guido Calabresi's 1970 book, *The Cost of Accidents*, provides a starting point for measuring the reasonableness of risk-taking. Calabresi argues that the overarching goal of tort law is to control the costs of accidents rather than to eliminate them. The negligent enabling tort will not eliminate cybercrime, but will reallocate the cost of these intrusions onto the software enterprises—the parties most capable of avoiding or minimizing the rate of computer intrusions.

The need for the proposed new tort may also be evaluated by comparing the radius of the risk to the cost of prevention.[234] Calabresi identified three types of costs that result from accidents: (1) primary costs, (2) secondary costs, and (3) tertiary costs.[235] In a computer software case, the primary or direct cost of a virus or other computer intrusion is likely to be borne by the user community. The primary costs of viruses include the financial resources and time spent in locating and removing virulent code from computer networks. Victims of identity theft suffer other primary costs from computer crime including damaged credit ratings and inability to secure loans.

---

231. CAL. CIV. CODE § 1798.82(b) (2005).

232. It is arguable that a company's violation of its duty to notify consumers of security breaches constitutes negligence per se. A company may defend against a negligence per se claim if the failure of notification was justified because notice would impede a pending criminal investigation. CAL. CIV. CODE § 1798.82(c) (2005).

233. Class Action Complaint, Hamilton v. Microsoft Corp., No. 49-031017-1010 (Cal. Super. Ct. Sept. 30, 2003).

234. *See generally* KOENIG & RUSTAD, *supra* note 118, at 47.

235. *Id*.

Secondary costs include the negative social impact of computer crimes and intrusions. The erosion of trust in the consumer market for online financial transactions, for example, may dissuade customers from providing credit card information for internet purchases.

Finally, Calabresi defined "tertiary" costs as the administrative costs of enforcing negligence liability and administering compensation for intrusions. Through adhesion license agreements, the software industry has succeeded in shifting all three varieties of costs onto the user community.

Almost no empirical data has been collected on even the primary costs of computer intrusions, so it may prove difficult to evaluate the radius of the risk created by insecure software. Similarly, no reliable data exists on the probability of cybercrime, its severity, or the costs of minimizing intrusions, so it is difficult to determine the most efficient level of precaution. Nonetheless, the risk/utility model serves as useful heuristic device in setting the standard of care, despite the lack of reliable, empirical data.

Every software design decision incurs some risk, but not every risk creation reaches the level of negligence.[236] A software vendor should only be liable for those appreciable risks of harm that can be prevented at a reasonable cost. The Grand Canyon could be made safe for the occasional clumsy hiker that loses his footing by filling it in with foam rubber. Reducing the risk would, however, eliminate the utility of the Grand Canyon as a picturesque setting. This solution would also be excessively costly compared to the benefit.

5. Res Ipsa, Proof, and Circumstantial Evidence of Breach

The *res ipsa loquitur* instruction supplies a "missing fact that the defendant was negligent."[237] In medical malpractice cases, the patient who has unexpected and unexplained injuries in the wake of a routine operation would be foreclosed from reaching the jury without the burden shifting power of *res ipsa*.[238] Similarly, direct evidence of software negligence is often difficult to obtain because the vendor does not release the design features or source code of its products. Circumstantial evidence of software failure is frequently the only available proof of design flaws. The doctrine

---

236. A utility was not liable for the risk that water in the water main would freeze due to unprecedented cold snap, causing flooding of neighboring houses. Blyth v. Birmingham Waterworks, 11 Exch. 781, 784 (1856). One is liable only for appreciable risks of harm, which a reasonable person would take. *Id.*

237. Alabama Power Co. v. Berry, 48 So. 2d 231, 238 (Ala. 1950).

238. Ybarra v. Spangard, 154 P.2d 687, 688-91 (Cal. 1944) (invoking the doctrine of *res ipsa loquitur* in case where a patient suffers post-operative neck pain normally not associated with the procedure).

of *res ipsa loquitur* assists the plaintiff by supplying a fact that must have existed in the causal chain between the act or omission of a software vendor and the computer intrusion that caused damages to the plaintiff.[239]

The underlying rationale for extending *res ipsa* to defective software is the vendor's ongoing control of the instrumentality that caused the injury. The average consumer is not in a position to ascertain the true cause of the software failure or computer malfunction. The ability of cybercriminals to enter computer systems by exploiting a known vulnerability is the modern equivalent of a barrel of flour falling from a miller's window and striking a passerby.[240] However, a mere computer intrusion may not be as probative of negligence if the vulnerability was not reasonably foreseeable.[241]

A data intermediary such as a software vendor should not be liable for failing to prevent cybercrime on mere conjecture or the mere possibility of negligence. The vendor must be in exclusive control or *res ipsa* should not apply. If someone other than the vendor had as much opportunity to thwart the cybercriminal, it cannot be said that it is more probable than not that the defendant is responsible.[242] *Res ipsa* would not be available, for example, where a software licensee is in control of the software. Finally, this doctrine is limited to situations where there is no direct evidence of a software vendor or online intermediary's negligence. The decision to apply *res ipsa* is a policy driven doctrine based on the defendant's superior knowledge that should be applied only when it is fair to shift the burden of coming forward with evidence because key facts are under the defendant's exclusive control.

C. Factual Causation

In a negligent enabling case, a plaintiff will need to demonstrate a causal connection (cause-in-fact) between software defects and conse-

---

239. "The factfinder may infer that the defendant has been negligent when the accident causing the plaintiff's physical harm is a type of accident that ordinarily happens as a result of the negligence of a class of actors of which the defendant is the relevant member." RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 17 (Proposed Final Draft No. 1, Apr. 6, 2005). In order for bad software cases to fall within the doctrine of res ipsa, the harm must be within the "exclusive control" of the software vendor and physical harm must have resulted.

240. *See generally* Byrne v. Boadle, 159 Eng. Rep. 299 (Exch. 1863).

241. *See* Meiring de Villers, *Virus Ex Machina Res Ipsa Loquitur*, 2003 STAN. TECH. L. REV. 1, 17 (2003).

242. *See, e.g.*, Malvinci v. Stratfield, Motor Hotel, Inc., 538 A.2d 690, 693 (Conn. 1988) (finding that the question of whether the plaintiff's own voluntary action in adjusting a shower that burned him was problematic); Dermatossian v. N.Y. City Transit Authority, 492 N.E.2d 1200, 1204-05 (N.Y. 1986) (finding that plaintiff failed to meet the burden of proving that a defendant had exclusive control of a dangerous instrumentality).

quential or direct damages suffered. The plaintiff asserting a negligent enabling claim must prove that a software licensor's acts or omissions caused legally recognized damages by a foreseeable third-party cybercriminal. The "but-for" test would determine "whether the defendant's conduct was a cause in fact of the plaintiff's harm."[243] In a defective software case, the plaintiff would lose if she "would have suffered the same harm had the defendant not acted negligently [because] the defendant's conduct is not a cause in fact of the harm."[244] Multiple causes for a computer intrusion may exist. Under the traditional test, "redundant multiple causes would preclude liability under the 'but for' analysis."[245]

The *Restatement (Second) of Torts* adopted a "substantial factor" test that only requires that the defendant materially contribute to a computer intrusion or internet security breach.[246] It may be difficult to determine whether a software bug, security hole, or a misconfiguration was a "substantial factor" if the security breach was connected to multiple potential causes. Courts will grapple with the "cause-in-fact" problem when third party intruders exploit a variety of security holes on numerous different networks in order to harm internet users.[247]

D. Proximate Cause or Legal Causation

Judges typically use the concepts of foreseeability and risk to decide proximate cause issues.[248] Proximate cause rules for internet security may limit the gatekeeper's liability to potential plaintiffs depending upon the

---

243. DOBBS, *supra* note 80, at 409.

244. *Id.*

245. DIAMOND, *supra* note 172, at 202.

246. *Id.* at 203-04.

247. The fact that an injury occurred does not mean that an actor is negligent as injury may be the result of unavoidable error or acts of God. In order for negligence to occur, the plaintiff must prove by a preponderance of the evidence that the defendant breached a standard of care. Villers, *supra* note 241, at 5.

248. DOBBS, *supra* note 80, at 444. Proximate cause is a conceptual device for judges to reduce the scope of a defendant's liability. Under proximate cause, "a negligent defendant is liable for all the general kinds of harms he foreseeable risked by his negligent conduct and to the class of person he put at risk by that conduct." *Id.* The concepts of foreseeability and risk-creation are basic to the concept of proximate cause or legal causation in tort law. "Ominously, the argument for preferring "legal cause" over "proximate cause" is much easier to follow than the case for replacing "reasonable foreseeability" with result-within-the-risk language." Richard L. Cupp, Jr., *Proximate Cause, The Proposed Basic Principles*, 53 S.C. L. REV. 1085, 1090 (2002) (comparing proximate cause formulations to an uncrackable puzzle). One court poked fun at the abstract notion of proximate cause: "[T]here are clear judicial days on which a court can foresee forever . . . ." Thing v. La Chusa, 48 Cal. 3d 644, 668 (1989).

kinds of harm suffered.[249] Even if the plaintiff establishes actual cause, there may not be recovery if the causal relationship between the defendant's breach and the plaintiff's losses is too remote. Justice Benjamin Cardozo noted: "General definitions of a proximate cause give little aid. Our guide is the reasonable expectation and purpose of the ordinary businessman when making an ordinary business contract. It is his intention, expressed or fairly to be inferred, that counts."[250]

The law of torts has historically distinguished between cause-in-fact (or actual cause) and proximate cause. In a computer security case, the plaintiff must present facts and circumstances that will convince a jury that the cybercrime that caused the plaintiff's injury was facilitated by the data handler or software vendor. Finally, the plaintiff must demonstrate that damages flowed from the breach of the defendant's duty to protect her against cybercriminals or other unauthorized users.

In the absence of comprehensive empirical studies of the frequency and costs of computer intrusions, it may prove difficult to evaluate the radius of the risk created by insecure software. Courts are reluctant to hold a defendant liable where the damages are bizarre or remote.[251] Judges will need to draw the line of liability for the consequences of defective software.

---

249. Courts frequently use the concept of proximate cause to limit liability for negligently enabling the crimes of third parties. *See, e.g.*, McCarthy v. Olin Corp., 119 F.3d 148, 169 n.21 (2d Cir. 1997) (Calabresi, J., dissenting) ("In other words, could the defendant be held liable for the criminal acts of an intervener absent any direct relationship with the plaintiff . . . Historically, a majority of jurisdictions answered this question in the negative, finding either no duty or no proximate cause.").

250. Bird v. St. Paul F. & M. Ins. Co., 120 N.E. 86, 87 (N.Y. 1918).

251. The traditional common law made a defendant liable for all of "the direct consequences" of a negligent act. *See In re* Polemis, 3 K.B. 560 (1921). However, the modern theory of proximate cause limits duties to reasonably foreseeable consequences. Justice Cardozo's majority opinion in Palsgraf v. Long Island Railroad, 162 N.E. 99 (N.Y. 1928) argued that that "proof of negligence in the air will not do." Applying Judge Cardozo's test to software, courts would ask whether a "foreseeable" victim of a cybercrime was owed a duty of care. Judge Andrews's dissent took issue with Judge Cardozo's formulation of duty preferring the older concept of proximate cause. *Id*. at 102-04. Judge Andrews contended that proximate cause determinations were always a matter of "practical politics." *Id*. at 103. In the case of bad software, the issue is whether a vendor's negligence is the "proximate cause" of a victim of a computer intrusion. Judge Andrews's test depends upon a judge making societal evaluations as to the desirability of extending proximate cause to software transactions.

Without a proximate cause limitation, internet security breaches could create boundless liability.[252] At some point, a cause of an internet security breach is so remote that it would be unfair to impose liability. If terrorists had exploited a security hole in software to construct illicit communication channels to coordinate the attacks on New York City and Washington D.C., the security hole theoretically could be deemed a cause-in-fact of the billions of dollars in damages that occurred on September 11, 2001. A court would be unlikely to determine the insecure software a proximate cause of the thousands of deaths and destruction even if the security hole was a cause-in-fact of the attacks.

E. Damages

The predominant injury in a cybertort case will be a financial loss, dignitary injury, or invasion of privacy rather than personal injury or death.[253] The theft of credit card and bank account numbers, for example, is of grave concern because the victims include "buyers and sellers, intermediaries and service industries."[254]

In June 2005, plaintiffs filed a class action lawsuit in California against CardSystems to force consumer notification when credit card information is hijacked by cybercriminals.[255] The merchants in CardSystems's network defended on the grounds that the complaint did not demonstrate any damages.[256] Because issuers absorbed all of the financial losses that resulted from fraudulent credit card transactions, the individual plaintiffs suffered no direct economic loss. Instead, the individual claimants argued that they had a reasonable apprehension that the security of their financial transactions had been compromised causing them "to lose control of [their] private financial information to a 'hacker.'"[257] The plaintiffs' claimed damages largely in the form of an anticipated loss much like claims for an enhanced risk of developing a future disease, where the injury has not yet manifested.[258]

The typical internet security case would not involve pain and suffering or general damages. A company could theoretically receive damages for

252. *See* DOBBS, *supra* note 80, at 445 (explaining how the proximate cause requirement of tort claims restricts liability).

253. *See* Savage, *supra* note 131.

254. Tom Zeller, *supra* note 98.

255. CardSystems Complaint, *supra* note 12; *see also* Evers, *supra* note 13.

256. *See* Evers, *supra* note 13.

257. CardSystems Complaint, *supra* note 12, at 3.

258. *See id.*; Metro North Commuter Railroad Co. v. Buckley, 521 U.S. 424, 444 (1997) (holding that the railroad workers who had chronic, unprotected exposure to asbestos dust had no claim for damages since no injury had yet appeared).

the unauthorized use of computer networks or be compensated for economic expenses incurred because of a computer virus. The law of torts may also provide for punitive damages to punish and deter software vendors that fail to remediate known vulnerabilities after many prior losses.

F. Defenses to Negligent Security Claim

Cybercrimes are frequently enabled by both the negligence of the vendor and the negligence of the consumer or user. In many instances, the virus problem is a self-inflicted wound because users fail to update their antivirus software.[259] An AOL survey found that one in seven users has no antivirus software at all.[260] Two-thirds of users did not have updated protection.[261] In many computer virus cases, the damaging code could be eliminated at either the computer network level or at the customer level by taking basic precautions. Downloading attachments or sharing diskettes without the user or the network incorporating the latest protection program, for example, may transmit viruses. The following Sections address three tort defenses and how they might apply in situations where user negligence also contributed to injury.

1. Contributory Negligence

In a contributory negligence jurisdiction, plaintiffs are precluded from any recovery if they contributed to the injury.[262] The defense of contributory negligence bars recovery entirely in claims where the plaintiff's own negligence contributed to the injury. The tort doctrine of avoidable consequences denies the recovery of damages that could have been avoided by the plaintiff's reasonable care. It is likely that contributory negligence in the form of user carelessness will be an issue in defective software cases. More than a third of a sample of nearly five hundred "users surveyed by the nonprofit National Cyber Security Alliance said they had a greater chance of winning the lottery or being struck by lightning than of being hit by malicious code."[263]

---

259. *Klez.H Epidemic: User Negligence or Failed Protection, About Antiviral Software*, ABOUT.COM, http://antivirus.about.com/library/weekly/aa030503a.htm (last visited Nov. 15, 2004).

260. Press Release, America Online, Joint AOL/NCSA Online Safety Study Finds That Computer Users Think They're Safer Than They Are, Nov. 19, 2004 (on file with author).

261. *Id.*

262. *See* RESTATEMENT (SECOND) OF TORTS §§ 463, 467 (1965).

263. *Study: Consumers Take Cyberattacks Lightly*, CNET NEWS.COM, Sept. 30, 2004, http://news.com.com/Study+Consumers+take+cyberattacks+lightly/2100-7349_

Contributory negligence may take the form of poor password security including weak passwords, accounts using default passwords, shared passwords, and the use of old versions of system software that enable packet sniffers to harvest access codes to compromise computer systems.[264] In cases of computer security, a user may carelessly fail to take reasonable precautions to protect his or her password or other confidential information. Computer users often place their passwords on their computers with Post-its, for example, which is tantamount to sharing the password with wrongdoers.

Users who choose passwords that are easy to guess should also be precluded from recovering from a software vendor even if it has a defect enabling cybercriminals. A user, who believes that his password has been stolen but does not change the compromised phrase, should also have no action for compromised accounts since his own negligence enabled privileged access to a vulnerable system. Similarly, a plaintiff should not be able to recover for permitting an intruder to exploit a password that has not been changed since installation.

For example, contributory negligence could be a defense in a defective software case assuming that a financial institution failed to implement reasonable methods to authenticate its customer's identity. A hospital could also be contributorily negligent if it fails to implement security solutions such as firewalls and routers. Therefore, contributory negligence could be a bar to recovery where a user's negligence contributed to the damage caused by exploiting vulnerable software.

2. Comparative Negligence

Most American jurisdictions have displaced contributory negligence with some form of comparative negligence. In a traditional contributory negligence jurisdiction, the plaintiff was precluded from any recovery if she contributed to the accident. In contrast, comparative responsibility statutes moderate the harsh "all of nothing" rule that provides no recovery for a plaintiff who is partially to blame.[265] In a comparative negligence jurisdiction, the negligence of the defendant is weighed against that of the plaintiff. A plaintiff in a negligent enablement case would have her dam-

---

3-5390749.html (reporting survey of 493 PC users surveyed by the nonprofit National Cyber Security Alliance).

264. SEI, CERT Coordination Center, UNIX Configuration Guidelines, http://www.cert.org/tech_tips/unix_configuration_guidelines.html (last visited Sept. 25, 2005).

265. Thomas R. Trenkner, Annotation, *Modern Development of Comparative Negligence Doctrine Having Applicability to Negligence Actions Generally*, 78 A.L.R.3d 339 (1977).

ages diminished by the degree of her own negligence, as compared to a contributory negligence regime, which would bar her relief entirely. A plaintiff's contributory negligence, therefore, would be a partial defense to a negligent enablement lawsuit based upon defective software.

Comparative negligence jurisdictions may be classified as employing either "modified" or "pure" versions.[266] In a modified system, negligent plaintiffs may recover, provided their negligence is neither equal to nor greater than that of the defendant. In a pure comparative negligence regime, plaintiffs' recovery is diminished by the degree of negligence, even if their negligence is greater than or equal to that of the defendant.

A plaintiff's failure to use standard antiviral software, for example, might constitute comparative negligence in a lawsuit over the transmission of software containing a virus. Also, harms enabled by input errors in online transactions will typically be the responsibility of the customer, not the online intermediary. An online banking website would likely not be responsible for a customer's misuse of services that resulted in financial injuries. Comparative negligence permits blame to be apportioned between the vendor and the user. Finally, in considering how to apportion fault, an efficient negligent enablement regime will allocate blame to the least cost avoider.

3. Assumption of Risk

Generally, if a plaintiff expressly or impliedly consents to confront the harm from a particular risk created by the defendant, she assumes the risk and is barred from recovery.[267] This defense is based on the public policy concern that the defendant should be relieved of his obligation to take reasonable care where the plaintiff "agrees to take his chances as to injury from a known or possible risk."[268] If a software licensor, for example, warns the user that it does not employ standard security devices in their operating system, a plaintiff may have voluntarily assumed a known risk. The express assumption of risk will likely have a continuing vitality in software license agreements, and express assumption of risk is a complete bar to recovery where it is allowed.

Mass market license agreements use exculpatory clauses to release the vendor from liability for all consequential damages resulting from negli-

266. *Id.*

267. Schutkowski v. Carey, 725 P.2d 1057, 1059 (Wyo. 1986) ("Exculpatory clauses releasing parties from liability for injury or damages resulting from negligence will be enforced if clause is not contrary to public policy.").

268. RESTATEMENT (SECOND) OF TORTS § 496A (1965).

gent software design.[269] The California Supreme Court in *Tunkl v. Regents of University of California* describes the factors a court will weigh before refusing to enforce an exculpatory clause on public policy grounds.[270] The court there reasoned that activities that are important to the public were of practical necessity and could not be the subject of bargaining.[271] Thus, where a party offered essential services, exculpatory clauses were less likely to be enforceable.[272] The *Tunkl* factors support refusing to recognize the affirmative defense of assumption of risk for negligently-designed software. The risk of preventable software design flaws carries substantial public policy implications and is likely not comparable to an individual's choice to assume the risk of an inherently dangerous recreational activity. What is appropriate for hazardous recreational activities should not apply to software that is critical to America's economic infrastructure and national security.

Courts should not enforce exculpatory clauses releasing vendors from liability for injuries or damages from negligent design because permitting this irresponsible behavior harms the public interest. The typical mass market license agreement seeks to eliminate the vendor's liability for negligent acts. Public policy should disfavor these clauses and closely scrutinize them, because the software industry should be liable for personal injuries or property damages resulting from negligent design.

Releases for hazardous recreational activities are often accompanied with warnings about the danger involved. In contrast, software users often do not receive such warnings and may even be lulled into complacency through advertisements promising complete computer security.

G. Policy Justifications for the Negligent Enablement Tort

New torts succeed because they are anchored to well-established principles of the common law.[273] During the 1960s and 1970s, new tort actions evolved to compensate the victims of wrongful discharge and defective products.[274] Our proposed negligent enablement tort is anchored in principles of premises liability, product liability, and warranty.

---

269. The exculpatory language in M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000) is emblematic of the industry standard that attempts to disclaim all liability for the vendor's negligent acts.

270. 60 Cal. 2d 92, 98-101 (1963).

271. *Id.*

272. *Id.*

273. Bernstein, *supra* note 81, at 1547.

274. *See generally* Anita Bernstein, *Muss Es Sein? Not Necessarily, Says Tort Law*, 67 LAW & CONTEMP. PROBS. 7 (2004) (arguing that these new causes of action in tort law were successful unlike many other new torts).

The premises liability concept that landowners who open their land to the public must use reasonable care, applies equally well to the intangible and ethereal world of cyberspace. The negligent enablement of cybercrime tort is a natural extension of the requirement that landowners, common carriers, innkeepers, and places of public entertainment owe affirmative duties of reasonable care to protect their customers. Just as landowners may create dangerous conditions that attract robbers and murderers, vendors of defective software create foreseeable risks to users. Courts have imposed liability upon physical businesses when crimes against customers are foreseeable and when the proprietor reasonably could have prevented the crime. The foreseeability of cybercrime creates a similar duty for the software industry.

Software that meets a reasonable safety standard will only become the norm if courts impose a duty to protect users from cybercriminals. Software that has been rushed to market without adequate testing may be cheaper to produce, just as brakeless cars are less expensive, but either marketing plan poses unacceptable risks to the user. Prior to the development of strict product liability, automobile manufacturers used contract disclaimers to disclaim all meaningful warranties and exclude consequential damages.[275] The American automobile industry blamed the epidemic of severe injuries on driver error or bad roads to deflect attention away from design defects that created excessive preventable dangers.[276]

In the 1950s and 1960s, automobiles were not equipped with seatbelts nor were they crashworthy for foreseeable collisions because Detroit's designers focused on aesthetics over safety.[277] Rigid steering wheel columns crushed chests and tattooed drivers with imprints of decorative but sharp emblems. Today's automobiles are much safer – product liability exposed such flaws and encouraged the auto industry to adopt improved designs. It is now time to extend these salutary principles of tort law to insecure software that facilitates the ability of third party cybercriminals to prey upon travelers on the internet.

The new negligent enablement tort will create essential incentives for the development of a seamless internet security system by imposing a fortified duty of care on the software industry. Software vendors should be

---

275. *See, e.g.*, Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 74 (N.J. 1960) (noting that the standard automobile sales contracts of Plymouth's automobiles included provision in fine print disclaiming all "warranties, express or implied, *made* by either the dealer or the manufacturer on the motor vehicle, chassis, or parts furnished") (emphasis in original).

276. *See* RALPH NADER, UNSAFE AT ANY SPEED (1965).

277. *Id.* at 112-28.

held liable when they knowingly market defective products and services that pave the way for highly foreseeable computer crimes. Just as the automobile industry enacted safety audits after the imposition of product liability, the software industry will respond to the proposed tort by allocating more resources to preventing cybercrime through better design, fortified product warnings, and more thorough testing. Software vendors owe a duty to warn consumers and other users of the potential threats to the security of their computer systems as well as providing information about how to avoid or recover from foreseeable computer intrusions. Requiring companies to transmit post-marketing warnings of software vulnerabilities will reduce the radius of the risk of computer intrusions.

The consumer orientation of modern product liability law inspires the negligent enablement tort. Prior to the development of strict product liability, automobile manufacturers used contract law as a means of shifting losses to their testimonies by contracts that limited consequential damages and disclaimed all warranties. Privity of contract shielded manufacturers from personal injury lawsuits stemming from dangerously defective products.[278] The breakthrough in product liability came when courts abandoned contract in favor of tort remedies for the injured consumers.[279]

The negligent enablement tort is necessary because of the failure of contract to provide minimum consumer protection to users. In the early 1960s, the courts supplemented remedies under warranty law with strict product liability.[280] A claimant in a product liability case can file suit in either warranty or tort.[281] Despite the strong temptation to transplant strict product liability into software transactions, two obstacles discourage such a development. First, contemporary product liability law is experiencing a pronounced shift away from absolute liability back to negligence. Second, the economic loss rule prevents courts from finding liability where the victim incurs economic harm, but no physical injury or death.[282] However, cybercrime enabled by defective software may cause damage to property other than the defective software where, for example, credit card numbers

278. The decision of Winterbottom v. Wright, 152 Eng. Rep. 402 (1842) was the landmark decision ruling that a passenger injured by a defective stagecoach had no standing to sue the repairer of the vehicle since the victim was not "in privity."

279. MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1915) (turning away from the privity approach).

280. RESTATEMENT (SECOND) OF TORTS §402(A) (1965).

281. *See, e.g.*, Castro v. QVC Network, Inc., 139 F.3d 114 (2d Cir. 1998).

282. Most courts determine whether a tort remedy is possible based upon the type of injury. If the software failure causes only economic loss, then no tort action may be filed. *See* Savage, *supra* note 131. Following this analysis, a tort remedy is only appropriate where physical injury or death arises out of the malfunctioning of software. *See id.*

of consumers or personal data are misappropriated. Courts will be more receptive to imposing liability with fault where the license agreement gives what is, in effect, an anti-warranty and remedy. Where pure economic damages are not recoverable under UCC Article 2 or UCITA, the negligent enablement tort is not displacing contract, but merely filling a void. Stronger warranty protection for software users will be necessary to ensure that the courts will not be flooded with negligent enablement claims.

Our proposed tort of negligent enablement of cybercrime tort is a logical extension of product liability law. The insecure software problem places an economic roadblock in the path of American competitiveness. At present, the software industry has shifted the cost of insecure software onto the user community. The tort of negligent enablement and fortified warranties will place the cost of injury on the party in the best position to prevent cybercrime. The negligent enablement tort will also reward socially responsible software vendors, who are currently at a competitive disadvantage. Our proposed tort will therefore reduce the rate of injuries from viruses, identity theft, computer intrusions, fraud, and other predatory online activities.

V. CONCLUSION

The rapid pace of technological change has exposed a fundamental weakness in the American civil justice system. In an era in which software "is becoming ubiquitous and increasingly complex[,] the importance of software [network, and internet] security is . . . growing exponentially."[283] At present, computer users have no meaningful remedies for injuries such as the theft of personal data, computer viruses, or internet fraud enabled by software failure. With cybercrimes skyrocketing and an ever-increasing amount of sensitive information being exchanged on the internet, the development of robust and trustworthy computer systems is a necessity.

Widespread breaches of internet security result in a "massive loss of valuable time and resources, reduced productivity and lost revenue."[284] Negligently designed and implemented software that enables hackers and creators of viruses to exploit computer systems is the root of much cyber-

283. Press Release, Cigital, Reliable Software Technologies Discovers Security Flaw in Netscape Navigator (Dec. 15, 1999), http://www.cigital.com/news/index.php?pg=art&artid=26.

284. FINJAN SOFTWARE, COMBATING THE NEW GENERATION OF MALWARE: SPYWARE, PHISHING, AND ACTIVE CONTENT 5 (Aug. 2005), http://www.finjan.com/company/whitepapers/combating_malware_finjan.pdf.

crime and unwanted computer intrusions. New negligence-based remedies are necessary because the only available defendant is often the software publisher whose security holes enabled the crime or tort. More security-conscious network architects, software designers, and website developers are the solution. The tort of negligent enablement will encourage the software industry to institute computer security audits by providing incentives to improve the quality of their products.[285]

All social and commercial relationships depend upon trust.[286] Unless the growing flood of cybercrime is curbed, the internet will become a lawless, "wild West," with unnecessary barriers to conducting business. The judiciary needs to be bolder in carving out tort duties to compensate the victims of cyberwrongs where software companies are the least cost avoider. In the absence of liability for the negligent enablement of cybercrime, "immunity breeds irresponsibility while liability induces the taking of preventive vigilance."[287] Thus, the new tort of negligent enablement brings good sense to software law for the millennium.

285. Ajay Ayyappan, *UCITA: Uniformity at the Price of Fairness*, 69 FORDHAM L. REV. 2471, 2518 (2001).

286. *See generally* FRANCIS FUKUYAMA, TRUST: THE SOCIAL VIRTUES (1995).

287. Thomas F. Lambert, Jr., *Suing for Safety*, TRIAL, Nov. 1983, at 48.