Maryland Law Review

Volume 67 | Issue 2 Article 5

Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?

Michael D. Scott

TORT LIABILITY FOR VENDORS OF INSECURE SOFTWARE: HAS THE TIME FINALLY COME?

MICHAEL D. SCOTT*

---

* The author is professor of law at Southwestern Law School in Los Angeles. He is author of seven legal treatises in the information technology law field, including SCOTT ON INFORMATION TECHNOLOGY LAW (3d ed. 2007) and SCOTT ON OUTSOURCING LAW & PRACTICE (2006). The author would like to thank the Southwestern Law School faculty for their useful comments on earlier versions of this Article and Dean Bryant Garth and the Board of Trustees for their financial support for the research on this Article.

Software vendors often profess their dedication to security. History, however, suggests otherwise: the software market has failed to produce secure software.[1]

I. INTRODUCTION

Software vulnerabilities cost businesses and consumers tens of billions of dollars each year.[2] Every day brings news of freshly discovered security flaws in major software products.[3] While Microsoft, due to its prominence in the operating system market,[4] gets the brunt of the

1. Abner Germanow et al., *The Injustice of Insecure Software*, @STAKE, Feb. 2002, at 1, *available at* http://www.netsourceasia.net/resources/atstake_injustice.pdf.

2. *See* Quentin Hardy, *Saving Software From Itself*, FORBES, Mar. 14, 2005, at 60 (quoting an estimate that 60 billion dollars are spent annually identifying and correcting software errors).

3. *See* Bruce Schneier, *Foreword* to JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE xix, xix (2002) [hereinafter Schneier, *Foreword*] ("The average large software application ships with hundreds, if not thousands, of security-related vulnerabilities.").

4. In February 2006, Windows XP held an 80.17% share of the operating system market, and all versions of Windows held a 95.28% share. Net Applications, Market Share (Feb. 2006), http://marketshare.hitslink.com/report.aspx?qprid=2 (follow "February 2006" current calendar month hyperlink). Some critics argue that the ubiquitous use of Windows itself leads to insecure systems due to the fact that Windows provides a common platform through which computer viruses and other harmful software can easily be spread. *See, e.g.*, DANIEL GEER ET AL., COMPUTER & COMMC'NS INDUS. ASS'N, CYBERINSECURITY: THE COST OF MONOPOLY 5 (2003), http://www.ccianet.org/papers/cyberinsecurity.pdf ("Most of the world's computers run Microsoft's operating systems, thus most of the world's computers are vulnerable to the same viruses and worms at the same time."). They argue that insecurity could be reduced by requiring heterogeneity in operating systems. *See id.* (emphasizing the necessity of diverse operating systems to protect critical infrastructure).

criticism for these flaws,[5] there are many other companies whose software is also targeted for security-related complaints.[6]

Yet, software vendors have traditionally refused to take responsibility for the security of their software, and have used various risk allocation provisions of the Uniform Commercial Code (U.C.C.) to shift the risk of insecure software to the licensee.[7] There were a few early cases in which licensees sought to have courts hold vendors liable for distributing defective software. These cases were unsuccessful.[8]

Since September 11, 2001,[9] increased attention has been given to the security of critical infrastructures,[10] including transportation, finance,[11] the power grid,[12] water supply and waste management sys-

---

5. *See, e.g.*, Brian Krebs, *Hackers Stepping Up Pace of Microsoft Exploits; Software Maker Responds With an Unusually High Number of Security Fixes*, WASH. POST, Oct. 13, 2006, at D01 (highlighting that Microsoft released dozens of security updates to Office within a single year); Robert McMillan, *Microsoft Bets Big on Vista Security*, COMPUTERWORLD, July 24, 2006, http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9001959 (noting that Microsoft XP had countless security problems, and that the newer Microsoft Vista may be even less secure); Jaikumar Vijayan, *Microsoft Releases Seven Security Patches*, COMPUTERWORLD, July 11, 2006, http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9001707 (detailing several security flaws in Microsoft products).

6. The CERT Coordination Center at Carnegie-Mellon University issues periodic Cyber Security Bulletins listing software vulnerabilities. *See* U.S. Computer Emergency Readiness Team, Cyber Security Bulletins, http://www.us-cert.gov/cas/bulletins (last visited Feb. 20, 2008) (listing vulnerability summaries since 2004). Each weekly bulletin contains hundreds of listings regarding a variety of vendors and products.

7. *See infra* Part I.D. While this Article focuses on the liability of software vendors to their licensees, an equally important issue is the liability of software vendors to third parties injured by insecure software, such as consumers whose personal information is obtained by hackers exploiting weaknesses in a vendor's software.

8. *See, e.g.*, Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 479 F. Supp. 738, 740–41 & n.1 (D.N.J. 1979), *aff'd in part, remanded in part on other grounds*, 635 F.2d 1081 (3d Cir. 1980) (finding no basis for imposing tort liability for breach of the commercial contract and rejecting plaintiff's claim for a new tort called "computer malpractice").

9. While the events of September 11th brought into sharp relief the government's failure to secure the airline transportation system, concerns about network security were expressed far earlier. For example, in 1994, a report from the Joint Security Commission to the United States Central Intelligence Agency and the Department of Defense stated: "[T]he security of information systems and networks [is] the major security challenge of this decade and possibly the next century." JEFFREY H. SMITH ET AL., JOINT SEC. COMM'N, REDEFINING SECURITY 2 (1994), *available at* http://www.loyola.edu/dept/politics/intel/jsc-report.pdf.

10. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999) (noting that the global community's growing dependence on computers and networks has created a significant vulnerability because "computer networks underlie key societal functions as diverse as finance, military command and control, medical treatment, and transportation.").

11. *Id.* at 894–95, 895 n.29.

tems,[13] computer networks,[14] military,[15] and homeland security and disaster recovery,[16] to name but a few.[17] These sectors "are increasingly dependent on the evolving information infrastructure,"[18] which in turn is increasingly dependent on secure software.[19] The growing risks inherent in insecure information technology systems have

12. *See, e.g.*, Dan Verton, *Software Failure Cited in Blackout Investigation; Task force points to malfunction at FirstEnergy site*, COMPUTERWORLD, Nov. 24, 2003, at 6, http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,87491,00.html (reporting that a utility company's software failure "may have contributed significantly" to the August 2003 blackout that affected the Northeast United States); *see also* U.S. NUCLEAR REGULATORY COMM'N, NRC INFORMATION NOTICE 2003–14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION 1 (2003), *available at* http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf (warning nuclear power reactor licensees about potential vulnerability to plant network servers).

13. *See* Tony Smith, *Hacker Jailed for Revenge Sewage Attacks*, THE REGISTER, Oct. 31, 2001, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage (detailing how a disgruntled employee hacked into the computer network of an Australian waste management system, causing raw sewage to flood local parks, rivers, and hotels).

14. *See* Bruce Schneier, *Blaster and the Great Blackout*, SALON.COM, Dec. 16, 2003, http://dir.salon.com/story/tech/feature/2003/12/16/blaster_security/index.html (reporting recent instances of business and government computer networks being attacked by worms and viruses).

15. *See* NANCY R. MEAD, INTERNATIONAL LIABILITY ISSUES FOR SOFTWARE QUALITY 29 (Carnegie-Mellon Univ., Special Report CMU/SEI-2003-SR-001, 2003), http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03sr001.pdf (warning that government and military computer networks are susceptible to attacks, particularly as the government increasingly relies on commercial platforms and software to contain costs).

16. *See* Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 408 (2007) (suggesting that the United States consider cyber attacks on critical information infrastructure as a national security matter rather than a criminal matter to protect the nation from threats of mass destruction and terrorism).

17. ERIC A. FISCHER, CONG. RESEARCH SERV., CREATING A NATIONAL FRAMEWORK FOR CYBERSECURITY: AN ANALYSIS OF ISSUES AND OPTIONS CRS–1 (2005) [hereinafter CRS] (analyzing the effectiveness of increased government attention to flaws in computer systems and associated infrastructure).

18. NAT'L RESEARCH COUNCIL, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 1 (Stewart D. Personick & Cynthia A. Patterson eds., 2003) [hereinafter CRITICAL INFORMATION].

19. *See generally* THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, at xi (2003), *available at* http://www.whitehouse.gov/pcipb [hereinafter NATIONAL STRATEGY] (identifying software vulnerability reduction and remediation as one of eight major initiatives for creating a more secure cyberspace). As noted by FBI Director Robert Mueller, "[t]oday a command sent over a network to a power station's control computer could be just as deadly as a backpack full of explosives." *FBI Director Says Businesses Reluctant to Report Cyber Attacks*, SAN JOSE MERCURY NEWS, Aug. 9, 2005.

prompted corporate executives,[20] computer security experts,[21] commentators,[22] lawyers,[23] and government officials[24] to call for action.

The collapse of Enron, Tyco, and a number of other major corporations, and the fraud uncovered in the aftermath, led Congress to take a first step. In 2002, Congress enacted the Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act,[25] which, *inter alia*, requires corporate executives to certify that their computer systems are secure.[26] This has placed corporate executives in the untenable position of having to certify that their computer systems are secure (with the prospect of massive fines and a long prison sentence if they are wrong),[27] while the vendors of the software used on those systems have no obligation, legal or otherwise, to certify that their products are secure.

---

20. *See* Douglas A. Barnes, *Deworming the Internet*, 83 TEX. L. REV. 279, 327–28 (2004) (calling for "lemon laws" for software); Gene J. Koprowski, *The Web: Dealing with Cyber-Crime*, UPI, Feb. 16, 2005 (noting that some technology executives are pressuring the White House to create a commission on cyber crime); Meridith Levinson, *Let's Stop Wasting $78 Billion a Year*, CIO MAGAZINE, Oct. 15, 2001, *available at* http://www.cio.com/article/30599/SOFTWARE_DEVELOPMENT_Let_s_Stop_Wasting_Billion_a_Year (noting that some CIOs are opting to use renewable licensing agreements or open-source technologies to avoid pitfalls associated with bad software).

21. Gary Anthes, *The Dark Side—Looming Threats for the Future of IT*, COMPUTERWORLD, Mar. 7, 2005, http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=100176 (blaming big software vendors for the "sometimes deplorable quality of commercial software"); CRS, *supra* note 17, at 14 ("[T]he vulnerabilities of computer operating systems . . . are among the most widely reported and exploited.").

22. *See, e.g.*, Bill Thompson, *Taking on Software Liability*, BBC NEWS, Oct. 7, 2005, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/technology/4318502.stm (calling for software firms to improve their code and accept liability for the failure of their products).

23. *E.g.*, Condron, *supra* note 16.

24. *E.g.*, DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 13 (2006), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (setting forth the federal government's plan to fund and protect critical infrastructure by enhancing cyber security and reducing cyber risk); Robert Lemos, *Security Czar Points Finger of Blame*, CNET NEWS.COM, July 31, 2002, http://news.com.com/2100-1001-947409.html?tag=fd_top (reporting that a presidential advisor recently criticized the software industry's apathy toward cyber security); Anne Saita, *Government Flexes Its Spending Muscle with "Model Contract,"* SEARCHSECURITY.COM, Sept. 24, 2003, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929141,00.html (explaining the new government-mandated "model contract" that requires vendors to meet specific security requirements).

25. 15 U.S.C. §§ 7201–7266 (Supp. IV 2001–2005) [hereinafter Sarbanes-Oxley Act or SOX].

26. While the intent of the SOX provisions was to place an obligation on publicly traded corporations to secure their systems against internal financial manipulation and fraud, the requirements of the Act also have the unintended, but salutary, side effect of requiring companies to secure their systems against other types of criminal activities, including cyberterrorism.

27. 18 U.S.C. § 1350(c) (Supp. IV 2006).

Why aren't software vendors being held liable for distributing insecure code? Why haven't current laws regarding negligence, product liability, and/or professional malpractice been applied to the developers of insecure software? Is this situation likely to change? These questions and others are explored in this Article.

A. What is Software?

For the purpose of this Article, *software* is defined as "[a] set of computer programs, procedures, and possibly associated documentation concerned with the operation of a data processing system, e.g., compilers, library routines, manuals, circuit diagrams."[28]

Software can be subdivided into operating system software and applications software.[29] Both of these categories have a wide range of definitions.[30] However, for the purpose of this Article, the term *operating system software* (or *operating system*) is defined as "a software program that controls the allocation and use of computer resources (such as central processing unit time, main memory space, disk space, and input/output channels)."[31] The operating system "essentially serves as the liaison between the applications software and the hardware."[32]

Application software relies on the operating system to perform many of its functions and is often viewed metaphorically as sitting "on top of" the operating system.[33] Applications are essentially "programs that permit a user to perform some particular task such as word processing, database management, or spreadsheet calculations, or

---

28. U.S. COPYRIGHT OFFICE, COMPENDIUM OF COPYRIGHT OFFICE PRACTICES II, 300–34 (1984). This is somewhat of a middle-of-the-road definition, more inclusive than those definitions limited only to the program code and less expansive than those definitions that include virtually everything but the hardware. *See, e.g.*, Mgmt. Sys. Assocs., Inc. v. McDonnell Douglas Corp., 762 F.2d 1161, 1163 n.2 (4th Cir. 1985) ("Software is . . . define[d] as everything that is not hardware."); Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37, 43 (D. Mass. 1990) ("[S]oftware includes one or more computer programs . . . along with . . . instruction manuals and 'templates' . . . .").

29. MICHAEL D. SCOTT, INTERNET AND TECHNOLOGY LAW DESK REFERENCE 39–40, 643–46 (7th ed. 2005).

30. *Id.*

31. United States v. Microsoft Corp., 65 F. Supp. 2d 1, 3–4 (D.D.C. 1999); *see also* Innovation Data Processing, Inc. v. IBM, Corp., 585 F. Supp. 1470, 1472 (D.N.J. 1984) ("An 'operating system' is a set of computer programs which guide and control the basic function of a computer.").

32. *In re* Data Gen. Corp. Antitrust Litig., 490 F. Supp. 1089, 1098 (N.D. Cal. 1980).

33. ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310, 1318 (N.D. Ill. 1990) ("Additional programs are . . . written to be used 'on top of' the operating system.").

that permit a user to play video games."[34] An application program "is generally any computer program which is not a systems program."[35]

Software security can be built into the operating system[36] or provided by separate application programs,[37] or both.[38] This Article focuses on operating system software and security-related application software.

To preserve the integrity of the software, and to make it difficult for competitors[39] and hackers[40] to discern how the program works, most software is distributed in object code[41] form. This is because "[t]he binary code or machine code (or object code) is virtually unintelligible to programmers."[42] In many cases, however, hackers have been able to penetrate computer systems by taking advantage of defects in the operating system or security software, and engaging in malicious activities even without deciphering the object code or accessing the source code.[43]

---

34. Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37, 43 (D. Mass. 1990).

35. Computer Scis. Corp. v. Comm'r of Internal Revenue, 63 T.C. 327, 329 (1974).

36. *See, e.g.*, Microsoft Corp., Windows XP Service Pack 2 Overview (Aug. 4, 2004), http://www.microsoft.com/windowsxp/sp2/overview.mspx (providing security updates for the Windows XP operating system).

37. *See, e.g.*, Addamax Corp. v. Open Software Found., Inc., 152 F.3d 48, 49 (1st Cir. 1998) ("[S]ecurity software is a component that can be used with the operating system to restrict outside access to sensitive information and to restrict a particular user to information consistent with that user's security classification.").

38. System security can also be built into the hardware; however, because this Article focuses on software security issues, hardware security issues are not discussed.

39. Software can qualify as a trade secret. *See, e.g.*, Avtec Sys., Inc. v. Peiffer, 21 F.3d 568, 575 (4th Cir. 1994) (stating that a trade secret can exist in source or object codes to computer programs).

40. For the purposes of this Article, a hacker is "an individual who accesses another's computer system without authority," Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 435 n.2 (W.D. Tex. 1993), and uses that unauthorized access to injure others. *See* United States v. Scott, 316 F.3d 733, 736 (7th Cir. 2003) (noting that hackers who use information gained via unauthorized access to the detriment of others may be punished).

41. Object code is "the version of a program in which the source code language is converted or translated into the machine language of the computer with which it is to be used." NAT'L COMM'N ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT 21 n.109 (1978), *available at* http://digital-law-online.info/CONTU/PDF/Chapter4.pdf.

42. United States v. Brown, 925 F.2d 1301, 1303 n.4 (10th Cir. 1991) (explaining that object code "is not discernible to even an expert programmer").

43. *See infra* note 52 and accompanying text.

B. What is Insecure Software?

The term *insecure software* has not been defined in any reported case or legislative enactment.[44] Even in the software and system security literature, the term is often used but never defined precisely.[45] A workable definition needs to take into account the problems that make software *insecure*. These include:

1. The existence in shipped software of *vulnerabilities*, namely, "flaw[s] in an information technology product that could allow violations of security policy";[46] and
2. The use of patches to fix known vulnerabilities.[47] A *patch* is a software module that is inserted into an existing program to fix an error or vulnerability. A patch may fix one security problem, but introduce another problem—sometimes security related, sometimes not.[48] The term patch reflects the fact that these software updates are no more than bandages, fixing only a narrowly prescribed problem with the software, and not always satisfactorily at that.[49]

Why are operating system and security applications software insecure? There are many reasons, including:

1. Competitive pressure to release new and updated products;[50]

---

44. A search of Westlaw indicates that the term has been used in only a single decision, but was not defined by the court. *See* Fed. Trade Comm'n v. Phoenix Avatar, LLC, No. 04 C 2897, 2004 WL 1746698, at *8 (N.D. Ill. 2004) (unreported decision) (noting that insecure software may allow spammers to access others' computers).

45. *See, e.g.*, Schneier, *Foreword*, *supra* note 3, at xix–xx (referring to "bad software," but failing to define the term).

46. William A. Arbaugh et al., *Windows of Vulnerability: A Case Study Analysis*, COMPUTER, Dec. 2000, at 52. "Antecdotal evidence alone suggests that known and patchable vulnerabilities cause the majority of system intrusions." *Id.*

47. *See* Ashish Arora et al., *Sell First, Fix Later: Impact of Patching on Software Quality*, 52 MGMT SCI. 465, 466 (2006) (explaining why a software vendor has an incentive to release a product with problems into the market and fix the problems afterwards).

48. "When companies try to fix programs, some 15% of newly introduced bugs aren't detected before release . . . . And when bugs are fixed, 7% of the repairs are faulty, with nearly half the new bugs capable of crippling an application or causing major errors." Steven V. Brull, *Then There's the Cost of Fixing the Fixes . . .*, BUS. WEEK, Dec. 14, 1998, at 40, *available at* http://www.businessweek.com/datedtoc/1998/981214.htm.

49. "Effectiveness of patches is somewhere between band-aids and a stiff drink." GERMANOW ET AL., *supra* note 1, at 4; *see also* Reid Skibell, *The Phenomenon of Insecure Software in a Security-Focused World*, 8 U. FLA. J. TECH. L. & POL'Y 107, 115 (2003) (stating that using patches means continually applying makeshift code, which often creates as many problems as it fixes).

50. *See* Bruce Schneier, *Liability and Security*, CRYPTO-GRAM NEWSLETTER, Apr. 15, 2002, *available at* http://www.schneier.com/crypto-gram-0204.html#6 [hereinafter Schneier, *Liability*] ("[T]he marketplace rewards low quality. More precisely, it rewards early releases at

2. Costs of development and testing,[51] and the impact of those costs on profits;[52]

3. Difficulties of testing for security vulnerabilities;[53]

4. Poor project management practices;[54]

5. Software and system complexity;[55]

6. Inability of customers to determine the existence of security vulnerabilities;[56] and

7. Lack of significant business[57] or legal[58] risks to the vendor in distributing insecure software.

---

the expense of almost all quality."); *see also* Skibell, *supra* note 49, at 113 (explaining that the effort expended on security flaws is often "proportional to the immediacy of the deadline").

51. *See* Schneier, *Liability*, *supra* note 50 ("The costs of adding good security [to software] are significant—large expenses, reduced functionality, delayed product releases, annoyed users . . . ."); *see also* GLENFORD J. MYERS, THE ART OF SOFTWARE TESTING 9 (Tom Badgett et al. eds., 2004) (noting that the fact that it is impractical or even impossible to find all of a program's errors impacts the economics of testing); Erin Kenneally, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, 26 LOGIN: MAG. OF USENIX & SAGE 62, 66 (2001), *available at* http://www.usenix.org/publications/login/2001-12/pdfs/kenneally.pdf (arguing that developers "invariably focus on business and technology concerns (functionality and time-to-market) at the expense of security . . . .").

52. Many commentators, however, argue that making software more secure is not that expensive. *See* Scott Berinato, *The Big Fix*, CSO MAG., Oct. 2002, *available at* http://www.csoonline.com/read/100702/fix.html (arguing that "90 percent of hackers tend to target known flaws in software" and "you can teach any freshman compsci student" to fix those flaws).

53. *See, e.g.*, Skibell, *supra* note 49, at 129 ("A conceptual reason why security testing is so difficult is namely that what one is trying to establish is the nonexistence of something.").

54. *See* JODY ARMOUR & WATTS S. HUMPHREY, SOFTWARE PRODUCT LIABILITY 13 (1993), *available at* http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr13.93.pdf (noting that over 80 percent of software organizations studied by Carnegie Mellon's Software Engineering Institute had very poor project management practices).

55. Arbaugh et al., *supra* note 46, at 52 ("Complex information and communication systems give rise to design, implementation, and management errors."); Bruce Schneier, *Software Complexity and Security*, CRYPTO-GRAM NEWSLETTER, Mar. 15, 2000, *available at* http://www.schneier.com/crypto-gram-0003.html (explaining that digital systems have gotten increasingly complex, resulting in less security).

56. *See* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 314–15 (2006) (describing the theory that suppliers have little incentive to "add high levels of security because the buyer has no low-cost method for ascertaining quality"); Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (2006), *available at* http://www.sciencemag.org/cgi/reprint/314/5799/610.pdf (same).

57. *See* Schneier, *Liability*, *supra* note 50 ("[T]he costs of ignoring security are minor: occasional bad press, and maybe some users switching to competitors' products. Any smart software vendor will talk big about security, but do as little as possible."); *see also* Skibell, *supra* note 49, at 129 (stating that the high cost of switching providers encourages companies to continue working with a provider even after learning of substantial security failings in their software).

These reasons create major impediments to efforts to compel software vendors to provide secure software.

C. Is Software a Good or a Service?

Whether software is a good or a service is a critical question when examining whether software should be the subject of product liability or professional malpractice claims.[59] That issue was hotly debated in the 1980s in the context of Article 2 of the U.C.C.[60]

Article 2 applies by its own terms only to transactions in goods.[61] The term *goods* means "all things [including specially manufactured goods] that are movable at the time of identification to a contract for sale."[62] To determine whether the U.C.C. applies to a particular computer transaction, it is necessary first to ascertain whether goods are involved.

Computer hardware, as a movable object, is clearly a good and thus subject to the provisions of Article 2.[63] Although hardware transactions often involve incidental services, such as installation, training, and maintenance, the presence of such services does not impair application of the U.C.C.[64] Transactions involving primarily personal services, however, such as those for maintenance, training, and support, are often held not to be goods, and thus not to fall within the U.C.C.[65]

---

58. *See* Kenneally, *supra* note 51, at 65 (explaining that software companies currently have no legal duty to take reasonable care to secure their products).

59. It is less of an issue in negligence law, because a claim can be based on negligent conduct as well as the negligent design or manufacturing of a product.

60. *See generally* Amelia H. Boss & William J. Woodward, *Scope of the Uniform Commercial Code; Survey of Computer Contracting Cases*, 43 BUS. LAW. 1513, 1514–15 (1988) (chronicling the discussions surrounding the application of the U.C.C. to intangibles such as computer programs).

61. U.C.C. § 2-102 (2007).

62. *Id.* § 2-103(k).

63. David A. Owen, *The Application of Article 2 of the Uniform Commercial Code to Computer Contracts*, 14 N. KY. L. REV. 277, 278 (1987).

64. *See* Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 479 F. Supp. 738, 742 (D.N.J. 1979) (finding that a software transaction was for the sale of goods, despite the inclusion of incidental services in the lease agreement); Dynamics Corp. v. Int'l Harvester Co., 429 F. Supp. 341, 346 (S.D.N.Y. 1977) (explaining that application of the U.C.C. depends on the "essence or main objective of the parties' agreement") (internal quotation marks omitted); Dreier Co. v. Unitronix Corp., 527 A.2d 875, 879 (N.J. Super. Ct. App. Div. 1986) (explaining that the sale of a computer is governed by the U.C.C., despite the fact that services are rendered as well).

65. *See* Heidtman Steel Prods., Inc. v. Compuware Corp., 178 F. Supp. 2d 869, 870 n.1, 871 (N.D. Ohio 2001) (U.C.C. does not apply to a series of contracts for the selection, modification, and installation of software); Conopco, Inc. v. McCreadie, 826 F. Supp. 855, 871 (D.N.J. 1993) (U.C.C. does not apply to consulting agreement for purchase of computer system); Computer Servicenters, Inc. v. Beacon Mfg. Co., 328 F. Supp. 653, 655 (D.S.C. 1970), *aff'd*, 443 F.2d 906 (4th Cir. 1971) (U.C.C. does not apply to data processing

Some courts, however, have been willing to apply the U.C.C. when a service contract also includes the sale of goods.[66] As the amount of goods involved in a service contract increases, the likelihood that the U.C.C. will be applied increases as well.

Major software transactions may involve the provision of both tangible property (e.g., the media on which the software is stored, documentation) and services (e.g., customization, installation, training, maintenance, support). The services inherent in off-the-shelf software that is bundled[67] with hardware are generally considered incidental to the goods aspect of the transaction, and the entire contract is deemed controlled by the U.C.C.[68]

The same is generally true for bundled, custom software: "Although the ideas or concepts involved in the custom designed software remained [the seller's] intellectual property, [the buyer] was purchasing the product of those concepts. That product required efforts to produce, but it was a product nevertheless and, though intangible, is more readily characterized as 'goods' than 'services.'"[69]

As a result, most contracts involving bundled software, either off-the-shelf or custom, fall within Article 2.[70] There is still a split of opin-

---

services); Geotech Energy Corp. v. Gulf States Telecomms. & Info. Sys., Inc., 788 S.W.2d 386, 388–89 (Tex. App. 1990) (U.C.C. does not apply to contract for installation and leasing of telephone system).

66. *See, e.g.*, Fed. Express Corp. v. Pan Am. World Airways, Inc., 623 F.2d 1297, 1300 (8th Cir. 1980) (applying the U.C.C. to portion of jet sales contract for training of crews); USM Corp. v. Arthur D. Little, Inc., 546 N.E.2d 888, 894 (Mass. App. Ct. 1989) (applying the U.C.C. to analyze a contract that involved software and services where the services were incidental).

67. "Bundling in the computer industry is a practice by which a computer manufacturer charges a single price for the hardware and software, and other services provided, along with the sale of the computer system." SCOTT, *supra* note 29, at 87–88.

68. *See, e.g.*, Carl Beasley Ford, Inc. v. Burroughs Corp., 361 F. Supp. 325, 334 (E.D. Pa. 1973), *aff'd*, 493 F.2d 1400 (3d Cir. 1974) (finding that the goods and services were virtually inseparable and allowing recovery of the entire bundled price under the U.C.C.); Nielson Bus. Equip. Ctr., Inc. v. Monteleone, 524 A.2d 1172, 1174–75 (Del. 1987) (determining that the consulting services that accompanied the purchase of a computer system were ancillary to the contract and could not be separated to avoid the implied warranties of the U.C.C.); Burroughs Corp. v. Joseph Uram Jewelers, Inc., 305 So. 2d 215, 215 (Fla. Dist. Ct. App. 1974) (applying the U.C.C. to a contract dispute against a provider for failing to properly program computer equipment); W.R. Weaver Co. v. Burroughs Corp., 580 S.W.2d 76, 81 (Tex. Civ. App. 1979) (finding that specific and comprehensive installation conditions may constitute evidence of an express warranty subject to the U.C.C.).

69. Triangle Underwriters, Inc. v. Honeywell, Inc., 457 F. Supp. 765, 769 (E.D.N.Y. 1978), *modified on other grounds*, 604 F.2d 737 (2d Cir. 1979).

70. See *supra* notes 66–69 and accompanying text; *see also* Commc'ns. Groups, Inc. v. Warner Commc'ns., Inc., 527 N.Y.S.2d 341, 344 (N.Y. Civ. Ct. 1988) (explaining that computer software is generally considered to be a tangible item and qualifies as a "good" under the U.C.C.).

ion on whether unbundled (standalone) software qualifies as a good because of its dominant service aspect,[71] although the majority of cases have held that the transaction is one for goods, governed by the U.C.C.[72]

D. The Application of Article 2 to Computer Software

The application of Article 2 to software transactions[73] offers vendors the opportunity to use the provisions of the U.C.C. to limit the

---

71. A few courts have held that custom programming is predominantly a service outside the U.C.C. *See, e.g.*, Wharton Mgmt. Group v. Sigma Consultants, Inc., 50 U.C.C. Rep. Serv. 2d 678, 681 (Del. 1990) (finding that the contract for the design of computer software was primarily for services, not goods, and thus, outside the scope of the U.C.C.); Data Processing Servs., Inc. v. L.H. Smith Oil Corp., 492 N.E.2d 314, 318 (Ind. Ct. App. 1986) (determining that the U.C.C. did not apply to a contract to "design, develop and implement an electronic data processing system"); Micro-Managers, Inc. v. Gregory, 434 N.W.2d 97, 98, 100 (Wis. Ct. App. 1988) (finding that a custom software design contract indicated the purchase of services, not goods, and thus the U.C.C. did not apply).

However, a growing number of courts have held that a software development contract is or may be a contract for goods governed by the U.C.C. *See, e.g.*, Micro Data Base Sys. v. Dharma Sys., Inc., 148 F.3d 649, 651, 654–55 (7th Cir. 1998) (finding that a contract for custom-made software and corresponding technological support fell into the U.C.C.); Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 675–76 (3d Cir. 1991) (finding software developed under a contract to be a good within the meaning of the U.C.C.); RRX Indus. v. Lab-Con, Inc., 772 F.2d 543, 546 (9th Cir. 1985) (finding that the U.C.C. controlled a transaction in which the sale of computer software dominated the service aspects of the contract); Colonial Life Ins. Co. v. Elec. Data Sys. Corp., 817 F. Supp. 235, 238–39 (D.N.H. 1993) (finding that the U.C.C. applied to sale of computer software where the contract also provided for years of servicing of the program); *see also* Downriver Internists v. Harris Corp., 929 F.2d 1147, 1151 (6th Cir. 1991) (declining to decide the question of whether software development contracts are goods for purposes of the U.C.C., "except to observe that genuine issues of material fact on the goods vs. services issue existed"); Harford Mut. Ins. Co. v. Seibels, Bruce & Co., 579 F. Supp. 135, 138 (D. Md. 1984) (denying a motion for summary judgment on the grounds that it is a question of fact as to whether software developed under contract is a good or service under the U.C.C.).

An ancillary question is whether a software license is equivalent to a sale. A majority of reported decisions have held that the fact that software is licensed does not preclude application of Article 2. *See* Stephen L. Sand, *Validity, Construction, and Application of Computer Software Licensing Agreements*, 38 A.L.R. 5th 1, 20–23 (1996) (listing cases in which courts held explicitly or implicitly that the U.C.C. applied to agreements involving computer software licenses).

72. *See supra* note 71 and accompanying text. For additional cases where courts found that software programs are goods, see Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 94 n.6 (3d Cir. 1991); Synergistic Techs., Inc. v. IDB Mobile Commc'ns., Inc., 871 F. Supp. 24, 29 n.7 (D.D.C. 1994); First Nationwide Bank v. Florida Software Servs., Inc., 770 F. Supp. 1537, 1543 (M.D. Fla. 1991); Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.2d 103, 108 n.4 (Tex. App. 2000); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305, 310 (Wash. 2000).

73. Whether Article 2 applies to software transactions has been an issue widely discussed in the literature. *See, e.g.*, Owen, *supra* note 63. For a decade, efforts were made to develop a new uniform contract law to apply to software and database transactions. Originally called U.C.C. Article 2B and then renamed the Uniform Computer Information

risks they assume in marketing their software products. These provisions include warranty disclaimers[74] and limitation of liability and remedies.[75]

1. Warranty Disclaimers

Despite the elaborate warranty provisions in the U.C.C.,[76] both express warranties and implied warranties can be disclaimed or modified by contract.[77] While warranty disclaimers are generally presumed valid,[78] such disclaimers "are construed strictly in favor of the buyer."[79]

No reported decision has unequivocally held that a software vendor has breached an express warranty.[80] There are three possible reasons for this:

> First, software manufacturers scrupulously avoid making express claims that software will perform any particular tasks, although they freely claim that their products have nearly mystical qualities. Secondly, any express promises are inevitably disclaimed in licensing agreements. Thirdly, it is generally agreed that software cannot be expected to perform

---

Transactions Act (UCITA), the drafting process became mired in controversy. *See* MICHAEL J. WALDMAN, NTS AM. JUR. 2D *Computers and the Internet* § 50 (2005) (generally discussing the UCITA); James S. Heller, *UCITA: Still Crazy After All These Years, and Still Not Ready for Prime Time*, 8 RICH. J.L. & TECH. 5 (2001) (chronicling the controversy surrounding the UCITA). After being adopted in only two states, Virginia, VA. CODE ANN. § 59.1-501.1 *et. seq.* (2006), and Maryland, MD. CODE ANN., COM. LAW § 22-101 (West 2002), the UCITA lost the support of its sponsoring organizations. *See* Patrick Thibodeau, *Sponsors Pull Support for Controversial UCITA Law*, COMPUTERWORLD, Aug. 1, 2003, http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,83676,00.html.

74. *See infra* notes 76–87 and accompanying text.

75. *See infra* notes 88–102 and accompanying text.

76. *See* U.C.C. § 2-312(1)(a) (2007) (implied warranty of title); *id.* § 2-313(1)(a) (express warranties); *id.* § 2-314 (implied warranty of merchantability); *id.* § 2-315 (implied warranty of fitness for a particular purpose).

77. *Id.* § 2-316; *see also, e.g.*, Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519, 528–29 (W.D. Pa. 2000), *aff'd*, 234 F.3d 1265 (3d Cir. 2000) (concluding that limitations on a license's warranty properly disclaimed the U.C.C.'s implied warranties of merchantability and fitness).

78. *See, e.g.*, Siemens Credit Corp. v. Marvik Colour, Inc., 859 F. Supp. 686, 694 (S.D.N.Y. 1994) (presuming that a waiver of warranties and consequential damages was valid).

79. LARY LAWRENCE, ANDERSON ON THE UNIFORM COMMERCIAL CODE 138 (West 2002 rev.) (1985); *see also* Sierra Diesel Injection Serv., Inc. v. Burroughs Corp., 874 F.2d 653, 658 (9th Cir. 1989) (noting that exclusions of warranties are generally construed against the drafter); Commc'ns. Groups, Inc. v. Warner Commc'ns., Inc., 527 N.Y.S.2d 341, 346 (N.Y. Civ. Ct. 1988) (invalidating the exclusion of a warranty because it was not conspicuous and the buyer was not notified that there was no implied warranty).

80. David Polin, *Proof of Manufacturer's Liability for Defective Software*, 68 AM. JUR. PROOF OF FACTS 3d. 333, 347 (2002).

perfectly, so such warranties as exist will be interpreted somewhat loosely.[81]

Courts generally uphold implied warranty disclaimers unless they are found to be unconscionable.[82] While courts are reluctant to apply the doctrine of unconscionability in the commercial context,[83] a warranty disclaimer has been found to be unconscionable where:

1. The contract is one of adhesion;
2. There is an inequality of bargaining power;
3. A complex piece of equipment is involved, about which the buyer has little knowledge to independently determine whether the equipment would fulfill the buyer's needs; and
4. The seller has expressly represented that the equipment is adequate.[84]

There is a split of authority as to whether or not warranty disclaimers must be made by each entity in the distribution chain in or-

---

81. *Id.*

82. U.C.C. § 2-302(1) (2004) provides that:

> If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.

See also Hartland Computer Leasing Corp. v. Ins. Man, Inc., 770 S.W.2d 525, 527 (Mo. Ct. App. 1989) ("Only such provisions of the standardized form which . . . are unexpected and unconscionably unfair are held to be unenforceable.").

In addition, courts generally will not allow the vendor to disclaim express warranties, particularly when they are included in the contract itself, finding that "a warranty disclaimer inconsistent with an express warranty is inoperative." L.S. Heath & Son, Inc. v. AT&T Info. Sys., 9 F.3d 561, 570 (7th Cir. 1993); *accord* Sierra Diesel, 890 F.2d 108, 113 (9th Cir. 1989) (finding that "warranty disclaimer clauses in printed form contracts were ineffective to avoid the express warranty").

83. JAMES J. WHITE & ROBERT S. SUMMERS, HANDBOOK OF THE LAW UNDER THE UNIFORM COMMERCIAL CODE § 4-9, at 172 (2d ed. 1980) ("In general, without a showing of procedural impropriety, courts will not invalidate in the name of unconscionability in commercial settings."); *see* Cryogenic Equip., Inc. v. S. Nitrogen, Inc., 490 F.2d 696, 699 (8th Cir. 1974) (finding disclaimer limiting remedies not unconscionable given expertise of parties and absence of evidence showing a disparity in bargaining power); Badger Bearing Co. v. Burroughs Corp., 444 F. Supp. 919, 923 (E.D. Wis. 1977) (rejecting a claim of unconscionability).

84. *See* A & M Produce Co. v. FMC Corp., 186 Cal. Rptr. 114, 126 (1982) (applying the doctrine of unconscionability to a complex transaction where the seller used a preprinted form agreement and had disparate bargaining power, and the sale resulted in allocating commercial risks in an socially or economically unreasonable manner). *See generally* John E. Murray, Jr., *Unconscionability; Unconscionability*, 31 U. PITT. L. REV. 1 (1969) (proposing a theoretical structure for unconscionability).

der to be effective.[85] Most courts require privity of contract for a disclaimer of implied warranties to apply.[86] Some courts, however, made no such requirement.[87]

2. Limitation of Liability and Remedies

The remedies available to a plaintiff for breach of warranty and the liability of the breaching party may be limited by contract.[88] One method of limitation is through the use of a liquidated damages provision.[89] Another method is to include within the contract a clause that: (1) provides a specific, exclusive,[90] limited remedy, such as repair or replacement of defective parts;[91] (2) limits the total liability of the vendor to a specific dollar amount, such as the total price paid on the

85. *See, e.g.*, Transp. Corp. of Am. v. IBM Corp., 30 F.3d 953, 958–59 (8th Cir. 1994) (finding that disclaimers extend to third party purchasers or end users); Prof'l Lens Plan, Inc. v. Polaris Leasing Corp., 675 P.2d 887, 898–99 (Kan. 1984), *aff'd*, 710 P.2d 1297, 1304 (Kan. 1985) (declining to extend the implied warranties of merchantability and fitness to non-privity manufacturers or sellers); Spagnol Enters., Inc. v. Digital Equip. Corp., 568 A.2d 948, 952 (Pa. Super. Ct. 1989) (explaining that privity is not required in suits between manufacturers and consumers for breach of warranty in Pennsylvania).

86. *See supra* note 85 and accompanying text; *see also* Barazzotto v. Intelligent Sys., Inc., 532 N.E.2d 148, 150 (Ohio Ct. App. 1987) (quoting 3 LARY LAWRENCE, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 2-316:155, at 232 (2002)) ("[T]he manufacturer's disclaimer of warranties does not run with the goods so as to protect any subsequent seller of them. To the contrary, each subsequent seller must make his own independent disclaimer in order to be protected from warranty liability."); *id.* at 151 (explaining that a retailer can be expected to know whether software will be fit for a particular use, at least to the extent of its compatibility with specific hardware, whereas a manufacturer cannot because it cannot know how the buyer plans to use the software).

87. *See, e.g.*, Spring Motors Distribs. v. Ford Motor Co., 489 A.2d 660, 663 (N.J. 1985) (holding that privity of contract with the remote supplier is not required for implied warranties); *Spagnol Enters.*, 568 A.2d at 952 (finding that privity is not required for suits between manufacturers and consumers).

88. U.C.C. §§ 2-316(4), 2-718, 2-719 (2004); *see also, e.g.*, AES Tech. Sys., Inc. v. Coherent Radiation, 583 F.2d 933, 939 (7th Cir. 1978) ("By limiting the warranties available and the remedies under the warranties, parties are able to provide a consensual allocation of risk in accordance with sound business practices."); NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536, 1542 (N.D. Okla. 1997) (explaining that Oklahoma law allows parties to limit remedies for breach of contract unless the terms are unconscionable).

89. U.C.C. § 2-316(4).

90. Unless a limitation provision is "expressly agreed to be exclusive," it is "optional." *Id.* § 2-719(1)(b); *see also, e.g.*, David Cooper, Inc. v. Contemporary Computer Sys., Inc., 846 S.W.2d 777, 779 (Mo. Ct. App. 1993) (noting that absent a specific provision that a 90-day provision is the only remedy, a buyer has a reasonable time to determine whether or not goods are defective).

91. U.C.C. § 2-719(1)(a); *see* Hunter v. Tex. Instruments, Inc., 798 F.2d 299, 302 (8th Cir. 1986) (upholding seller's ability to limit liability for breach of express warranties to repair or replace); Consol. Data Terminals v. Applied Digital Data Sys., Inc., 708 F.2d 385, 392 n.6 (9th Cir. 1983) ("A remedy limited to repair is not unconscionable per se."); Ritchie Enters. v. Honeywell Bull, Inc., 730 F. Supp. 1041, 1048 (D. Kan. 1990) ("The remedy of repair and replacement offers the seller an opportunity to cure defects and to

contract or the total amount paid during a specified time period;[92] or (3) limits the buyer to only direct damages[93] by excluding all special,[94] incidental,[95] or consequential[96] damages.[97]

At least in commercial transactions, liability limitation clauses "generally are valid and enforced by the courts."[98] However, such clauses must be carefully drawn because any ambiguity will be construed against the drafting party.[99] Furthermore, in addition to argu-

---

minimize its liability exposure and provides the buyer with goods which conform to the contract within a reasonable period of time.") (citation omitted).

92. *See* Brown v. SAP Am., Inc., No. C.A. 98-507-SLR, 1999 WL 803888, at *8–10 (D. Del. Sept. 13, 1999) (upholding a contract provision limiting seller's liability for losses to a refund of the license fees paid); Bridgestone/Firestone, Inc. v. Oracle Corp., 3 Computer Cas. (CCH) ¶ 46,519, at 63,437, 63,442 (N.D. Cal. 1991) (noting that consequential damages may be limited to a certain amount unless the limitation of exclusion is unconscionable); Garden State Food Distribs., Inc. v. Sperry Rand Corp., 512 F. Supp. 975, 978 (D.N.J. 1981) (holding damages for breach of warranty were limited to express contract terms which limited recovery to the price paid for the equipment).

93. Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473, 1488–89 (D. Minn. 1991) (holding that buyer's recovery was limited to direct damages); *see* Electro-Matic Prods., Inc. v. Creata Data, Inc., 1 Computer Cas. (CCH) ¶ 46,052, at 61,008, 61,009 (E.D. Mich. 1988) (same).

94. "[S]pecial damages are those that ensue, not necessarily or ordinarily, but because of special circumstances." Applied Data Processing, Inc. v. Burroughs Corp., 394 F. Supp. 504, 509 (D. Conn. 1975) (quoting Ruggles v. Buffalo Foundry & Mach. Co., 27 F.2d 234, 235 (6th Cir. 1928)).

95. U.C.C. § 2-715(1) (2004) (incidental damages "include expenses reasonably incurred in inspection, receipt, transportation and care and custody of goods rightfully rejected, any commercially reasonable charges, expenses or commissions in connection with effecting cover and any other reasonable expense incident to the delay or other breach").

96. *See id.* § 2-715(2) (consequential damages include "any loss resulting from general or particular requirements and needs of which the seller at the time of contracting had reason to know and which could not reasonably be prevented . . . and injury . . . proximately resulting from any breach of warranty"). Many courts have upheld the validity of contracts that exclude recovery of consequential damages for commercial loss. Transp. Corp. of Am. v. IBM Corp., 30 F.3d 953, 960 (8th Cir. 1994) ("An exclusion of consequential damages set forth in advance in a commercial agreement between experienced business parties represents a bargained-for allocation of risk that is conscionable as a matter of law."); D.S. Am. (E.), Inc. v. Chromagrafx Imaging Sys., Inc., 873 F. Supp. 786, 794 (E.D.N.Y. 1995) (noting that a contract may exclude consequential damages unless it is unconscionable); Wausau Paper Mills Co. v. Chas. T. Main, Inc., 789 F. Supp. 968, 975 (W.D. Wis. 1992) (same). *But see* St. John's Bank & Trust Co. v. Intag, Inc., 938 S.W.2d 627, 629 (Mo. Ct. App. 1997) (awarding consequential damages).

97. *See* Krider Pharmacy & Gifts, Inc. v. Medi-Care Data Sys., Inc., 791 F. Supp. 221, 224–26 (E.D. Wis. 1992) (finding that buyer's recovery was limited to direct damages because contract excluded liability for special, incidental, or consequential damages); Hi Neighbor Enters., Inc. v. Burroughs Corp., 492 F. Supp. 823, 826 (N.D. Fla. 1980) (same).

98. *See* Caudill Seed & Warehouse Co. v. Prophet 21, Inc., 123 F. Supp. 2d 826, 829 (E.D. Pa. 2000) (noting that liability limitations in commercial contracts are valid under Pennsylvania law).

99. *See* Consol. Data Terminals v. Applied Digital Data Sys., Inc., 708 F.2d 385, 392 (9th Cir. 1983) (determining that a clause that limited remedies to repair of defective equip-

ing ambiguity, an injured party can also claim that the limitation clause should not be enforced because it is unconscionable,[100] failed its essential purpose,[101] or was induced by fraud.[102]

While contract law sometimes provides a software licensee with a remedy against a software vendor, the vast majority of reported decisions have held instead that the risk allocation provisions of Article 2 will be applied, thereby limiting or barring recovery to the injured software licensee.[103]

II. APPLYING NEGLIGENCE LAW TO INSECURE SOFTWARE

"[M]any experts have suggested the use of tort law as a model for computer-related cases."[104] Indeed, some argue that those who develop software and computer systems are in the best position to take action to prevent security breaches,[105] and that the imposition of lia-

---

ment did not apply when the warranted goods failed to perform to specifications despite seller's efforts to repair); Lovely v. Burroughs Corp., 527 P.2d 557, 563 (Mont. 1974) (finding that a clause limiting consequential damages arising from delay in delivery did not bar recovery for losses due to product malfunction).

100. *See supra* notes 80–82 and accompanying text. *But see Consol. Data Terminals*, 708 F.2d at 392 n.6 ("A remedy limited to repair is not unconscionable per se.").

101. *See* Chatlos Sys. v. Nat'l Cash Register Corp., 635 F.2d 1081, 1086 (3d Cir. 1980) (determining that a contractual limitation to limit remedies to repairs was unenforceable because the remedy failed its essential purpose); Fargo Mach. & Tool Co. v. Kearney & Trecker Corp., 428 F. Supp. 364, 381–82 (E.D. Mich. 1977) ("Where such circumstances cause a limited remedy to fail of its essential purpose . . . the limitation of buyer's remedy to repair or replacement is inoperative . . . ."); *cf.* W.R. Weaver Co. v. Burroughs Corp., 580 S.W.2d 76, 82 (Tex. Civ. App. 1979) (declining to permit summary judgment in favor of buyer where buyer did not plead that his remedy was unconscionable or had failed in its essential purpose).

102. U.C.C. § 2-721 (2004) ("Remedies for material misrepresentation or fraud include all remedies available under this Article for non-fraudulent breach."); Am. Elec. Power Co. v. Westinghouse Elec. Corp., 418 F. Supp. 435, 460 (S.D.N.Y. 1976) ("[T]he contractual limitation of liability precluding the recovery of consequential damages cannot be effective if plaintiffs' claims of fraudulent inducement are sustained at trial.").

103. For instance, in *Mesa Business Equipment, Inc. v. Ultimate Southern California, Inc.*, No. 89-55825, 1991 WL 66272 (9th Cir. Apr. 30, 1991) (unpublished table decision), Mesa, an office supply company, claimed that defects in software provided by a computer vendor, Ultimate Corporation, caused it to go bankrupt. *Id.* at *1. Mesa sued in bankruptcy court for over $2 million in damages. *Id.* The Ninth Circuit agreed with the bankruptcy court judge that the warranty disclaimers in the contract precluded Mesa from recovering any money from the defendants. *Id.* at *4.

104. CRITICAL INFORMATION, *supra* note 18, at 3.

105. *See id.* at 3–4 ("The applicability of tort law and the potential for civil lawsuits and monetary damages could encourage companies to invest in computer security measures."); *see also* Kenneally, *supra* note 51, at 64–65 (positing that software manufacturers should be assigned a legal duty of reasonable care to maintain software security).

bility on developers will motivate them to create more secure software.[106]

There have been a number of class action suits filed against software vendors and software users for breaches of security, particularly where such breaches have exposed consumers' personal and financial data to criminals who, in turn, have used the data for identity theft and other financial crimes.[107] "Such plaintiffs may allege that vendors were negligent in their production or design of computer security systems, including . . . their coding of security and encryption software."[108] However, while negligence law is an attractive tool to use against software vendors who distribute insecure software,[109] it has some critical limitations.

First, to state a claim for negligence, a plaintiff must plead and prove that: (1) the software vendor owed a duty to the plaintiff; (2) the vendor breached its duty; (3) the breach of duty was a cause-in-fact of the plaintiff's injury; (4) the breach was a proximate cause of the plaintiff's injury; and (5) the plaintiff suffered compensable damages as a result of that breach.[110] Each of these elements creates challenges for a plaintiff seeking to hold a vendor liable for insecure software.

A. Duty

The first question is: what duty, if any, does a software vendor owe to a licensee to provide secure software? A duty of due care must exist

---

106. *See* Schneier, *Liability*, *supra* note 50 ("The engine of this [software security] improvement will be liability—holding software manufacturers accountable for the security and, more generally, the quality of their products—and the timetable for improvement depends wholly on how quickly security liability permeates cyberspace."); *id.* ("If we expect software vendors to reduce features, lengthen development cycles, and invest in secure software development processes, they must be liable for security vulnerabilities in their products."); *cf.* Jeffrey D. Neuburger & Maureen E. Garde, *Information Security Vulnerabilities: Should We Litigate or Mitigate?*, SOFTWARE L. BULL., Apr. 2004, at 3 (questioning the relationship between liability litigation and product improvement).

107. *See generally* Kevin P. Cronin & Ronald N. Weikers, *Liability for Data Security and Privacy Breaches*, 23 ANDREWS COMPUTER & INTERNET LITIG. REP. 11 (2005).

108. *Id.*

109. Negligence claims, for example, may be available in situations in which product liability claims may not be available. *See, e.g.*, Griggs v. BIC Corp., 981 F.2d 1429, 1439–40 (3d Cir. 1992) (holding that a design was not defective under product liability law, but a finding of negligence was possible); Tillman v. R.J. Reynolds Tobacco Co., 871 So. 2d 28, 34–35 (Ala. 2003) (finding that a cigarette smoker might recover in negligence, but could not recover under strict liability).

110. DAVID G. OWEN, PRODUCTS LIABILITY LAW § 2.1, at 61 (2005).

between the defendant and an injured party before liability can be imposed.[111]

With respect to insecure software, there are two possible duties of a vendor: (i) a duty to design and develop secure software; and (ii) a duty to instruct the licensee on "how to use its products safely and to warn them of hidden dangers that the products may contain."[112]

The existence of a duty "is largely a policy-based determination."[113] Determining the existence of a duty of a software vendor will require a court to balance a number of factors, including:

> the foreseeability of the harm of computer intrusions or other breaches of security, the degree of certainty between software vulnerabilities and harm, the closeness of 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 as well as insurance.[114]

It is generally foreseeable that any complex software will have "bugs."[115] The problem is that it is not foreseeable exactly what those bugs will be, or what the impact of those bugs will be on the licensee or a third party.[116] If these security problems were known to the ven-

---

111. Atlas v. Selwyn, 4 Computer Cas. (CCH) ¶ 46,834, at 65,112 (E.D.N.Y. 1993). According to the *Second Restatement of Torts*, duty:

> denote[s] the fact that the actor is required to conduct himself in a particular manner at the risk that if he does not do so he becomes subject to liability to another to whom the duty is owed for any injury sustained by such other, of which that actor's conduct is a legal cause.

RESTATEMENT (SECOND) OF TORTS § 4 (1965) [hereinafter SECOND RESTATEMENT].

The term *duty* "is particularly valuable in describing the requirement that action shall be taken for the protection of the interests of others. It is also useful to describe the requirement that the actor, if he acts at all, must exercise reasonable care to make his acts safe for others." *Id.* § 4 cmt. B.

112. OWEN, *supra* note 110, § 2.1, at 62–63.

113. JOHN L. DIAMOND ET AL., UNDERSTANDING TORTS § 8.01, at 118 (2d ed. 2000); *see also, e.g.*, NATIONAL STRATEGY, *supra* note 19, at 37 ("All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace.").

114. Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 519–20 (2006), *based upon factors set forth in* Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968).

115. *See* FREDERICK P. BROOKS, JR., THE MYTHICAL MAN-MONTH: ESSAYS ON SOFTWARE ENGINEERING 182–84 (1995) (discussing how the complexity of computer software leads to technical problems).

116. *See* Public Wiki, Criteria for a Lab to Certify Software, http://abstract.cs.washington.edu/wiki/index.php/Criteria_for_a_Lab_to_Certify_Software (last visited Feb. 20, 2008) (stating that bugs are often minor mistakes that "live in a huge sea of code, millions

dor, arguably, a reasonable vendor would attempt to fix them.[117] Today, while major vendors have undertaken programs to make their software more secure,[118] it is still often users and other organizations who first identify security flaws in software.[119] Even when a flaw is identified, it is not necessarily true that the vendor will fix it immediately (or at all).[120]

Because vendors (meaning developers and suppliers of the software) generally distribute only the machine-readable object code of their products,[121] they are the only ones who know the actual level of security of their software and, therefore, are the only ones who can isolate and repair the problems. Hence, it is argued, software vendors owe a duty to their licensees and to society as a whole to ensure the security of their software.[122]

B. Standard of Care

Even assuming that a duty is found, the next question is: What is the standard of care imposed on the software vendor by that duty? The amount of care and the type of conduct required will vary with the circumstances, but a general, objective standard of care, that is, what the reasonably prudent person would do under the circumstances, does not change.[123] As noted in a recent article:

---

of lines long for much commercial software, that is set up in untold numbers of different environments, with different configurations, different inputs and different interactions with other software"); *but see* Skibell, *supra* note 49, at 112 ("[S]ome of the most problematic security concerns are eminently foreseeable and may not have even been that difficult to fix.").

117. *But see* Kenneally, *supra* note 51, at 66 (explaining that software developers "invariably focus on business and technical concerns (functionality and time-to-market) at the expense of security. It is no secret that programmers have had the knowledge and ability to prevent many buffer overflow vulnerabilities choose not to because of business reasons.").

118. *E.g.*, Robert Lemos, *One Year On, Is Microsoft Trustworthy?*, CNETNEWS.COM, Jan. 23, 2003, http://news.com/2100-1001-981015.html.

119. *See* Ted Bridis, *Microsoft Admits Easy Hack for Passport Service*, PITTSBURGH TRIB. REV., May 9, 2003 (reporting that a security specialist found a major security flaw in Microsoft Passport in about four minutes); *see also supra* note 6 and accompanying text.

120. *See supra* note 117 and accompanying text.

121. *See supra* notes 41–42 and accompanying text.

122. It is generally conceded that the complexity of major software packages, and the variety of applications in which the software is used, makes it impossible for vendors to offer bug-free software. *See* BROOKS, *supra* note 115, at 183–84 (noting that complexity creates technical and management problems that make it difficult to find and destroy all bugs). However, that does not mean that they should not have a duty to use all means reasonably available to them to provide secure software. As noted by one commentator, "[t]he costs associated with insecure computers on the Internet weigh heavily in favor of assigning a duty to secure systems." Kenneally, *supra* note 51, at 64.

123. *See* SECOND RESTATEMENT, *supra* note 111, § 283 (establishing the "reasonable man" standard); *id.* § 296(1) (explaining that emergency situations factor into determining

> The standard of care with respect to claims related to security practices is evolving rapidly; methodologies, procedures, and practices have been accepted by the industry, and are continually being improved. The standard of care for security is a moving standard relative to the risks exposed.[124]

In *Invacare Corp. v. Sperry Corp.*,[125] a district court refused to dismiss a negligence claim alleging that a computer seller was negligent for recommending its program and services to the buyer when "it knew, or in the exercise of ordinary care, it should have known, that . . . the programs and related data processing products were inadequate,"[126] and because it advertised to the buyer when it knew or should have known that "the programs furnished could not satisfy [the buyer's] requirements."[127] Applying section 299A of the *Restatement* (*Second*) *of Torts*, the court held that personnel in the computer industry, like personnel in other trades, should be held to the ordinary standard of care for their trade.[128]

In the software context, "the appropriate level of care to be followed in developing a custom computer program . . . will vary depending on the nature and intensity of the perceived risk resulting from an error."[129] The software vendor's duty under negligence law is not perfection, but only reasonableness.[130] Thus, the software does not need to be error-free. It need only meet the standard of care of a

---

whether one acted as a "reasonable man under the circumstances"). Other Restatement provisions address the level of care owed by a member of a trade: "one who undertakes to render services in the practice of a profession or trade is required to exercise the skill and knowledge normally possessed by members of that profession or trade in good standing in similar communities." *Id.* § 299A; *see also* cmt. b. (explaining that section 299A is a special application of the reasonable man standard and noting that if an individual has "greater skill than that common to the profession or trade, he is required to exercise that skill . . . .").

124. Cronin & Weikers, *supra* note 107, at 11.

125. 612 F. Supp. 448 (N.D. Ohio 1984).

126. *Id.* at 453.

127. *Id.*

128. *Id.* ("If machinists, electricians, carpenters, blacksmiths, and plumbers, are held to the ordinary standard of care in their professions, *the Court fails to see why personnel in the computer industry should be held to any lower standard of care.* . . . Negligence in the business setting is clearly actionable.") (emphasis added).

129. 2 RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY § 10:30, at 10–81 (3d ed. 2006).

130. Software vendors argue, often successfully, that all software is subject to defects ("bugs"), and that software cannot be made perfect. While this may be true, it is not unreasonable to hold a vendor to a higher standard of care for software used in critical applications (e.g., network security) than software for video games or word processing.

reasonable vendor of security-related software under the circumstances.[131]

One key element in establishing a standard of care for secure software is to determine whether there is a custom or usage in the software industry regarding the security standards applicable to operating system and other security-related software. In assessing the proper standard of care, industry-wide practices should be reviewed. The term "best practices"[132] refers to those technical, business, and management practices that have proven successful and are used by a large number of companies in an industry. At a minimum,[133] implementing best practices in secure software development and testing[134] should be required to avoid a negligence claim.

However, a court may hold a defendant to a higher standard than that set by the industry if it finds that the industry standard is inadequate.[135] For example, in *The T.J. Hooper v. N. Barge Corp.*,[136] the owner of an oceangoing tugboat was found liable for the loss of barges

---

131. Kenneally, *supra* note 51, at 66 ("The standard of care/scope of the duty will depend on the quality and quantity of the measures needed to secure relative to the actor's ability to control, assumption of responsibility, and/or socioeconomic concerns.").

132. Paul Murphy, *Software Vulnerabilities and the Future of Liability Reform*, LINUXINSIDER, Jan. 22, 2004, http://www.linuxinsider.com/story/32660.html (remarking that best practices are not clearly defined: "The question, of course, is what constitutes a best practice, and the only answer I've ever found is that a best practice is whatever an expert witness . . . is likely to believe it to be.").

133. For example, some states grant the provider, via statute, an affirmative defense if the product was "state of the art" at a specified time, often the time of its initial sale. *See, e.g.*, ARIZ. REV. STAT. ANN. § 12-683(1) (2002) (allowing the use of a "state of the art" affirmative defense in product liability actions for inadequate design or fabrication); IND. CODE ANN. § 34-20-5-1(1) (LexisNexis 1998 & Supp. 2006) (establishing a rebuttable presumption that a product is not defective when it conforms with the generally recognized "state of the art"); IOWA CODE ANN. § 668.12(1) (West 1998) (providing a defense against product liability action where a product conformed to the state of the art when it was designed or created); NEB. REV. STAT. § 25-21,182 (1995) (establishing a defense against product liability action when a product at the time of sale conformed with the state of the art, defined as the "best technology reasonably available").

134. As noted in the Comments to the UCITA:

> A great deal of theoretical and practical work is currently focused on techniques to reduce the time and cost needed to determine program "correctness." Professional standards also exist for software quality evaluation. Commercially reasonable use of existing testing techniques can be one benchmark of whether a computer program is merchantable in law. As industry standards evolve, what constitutes a merchantable program will evolve along with those standards.

LORIN BRENNAN ET AL., THE COMPLETE UCITA § 403 cmt. 3(a) (2004).

135. *See* SECOND RESTATEMENT, *supra* note 111, § 295A ("In determining whether conduct is negligent, the customs of the community, or of others under like circumstances, are factors to be taken into account, but are not controlling where a reasonable man would not follow them.").

136. 60 F.2d 737 (2d Cir. 1932).

it was towing because of its failure to equip the tugboat with a radio that could receive weather forecasts.[137] The defendant presented evidence that the installation and use of a radio was not widely done in the maritime industry, and, therefore, its lack of a radio was consistent with the industry standard.[138] Rejecting that position, Judge Hand stated that "Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[139]

Thus, while "compliance with industry-wide standards is often an acceptable demonstration of due care,"[140] that is not always the case. As noted in *Northwest Airlines, Inc. v. Glenn L. Martin Co.*,[141] "the fact that Northwest conformed to the practice of other airlines in failing to equip [its planes] with radar did not establish its exercise of ordinary care as a matter of law. Customary practice is not ordinary care; it is but evidence of ordinary care."[142]

Industry-standard software development and testing practices may provide a baseline for determining the requisite standard of care for the developer of security-related software, but they do not necessarily establish the actual standard of care that a vendor must meet. The potentially catastrophic losses that may result from use of insecure software encourage a significantly higher standard of care for software development in this area. The exact standard of care must be determined on a case-by-case basis.

C. Breach of Duty

Once it has been shown that the defendant owed a duty of due care to the plaintiff, it is then necessary to establish that the defendant breached that duty by an act or omission that exposed the plaintiff to an unreasonable risk of harm, that is, that the defendant acted negligently.[143] "The breach of a duty . . . does not make the actor liable. It

---

137. *Id.* at 737, 740. *But see* Hendry Corp. v. Aircraft Rescue Vessels, 113 F. Supp. 198, 201 (E.D. La. 1953) (finding that the mere absence of a radio does not make a tug unseaworthy).

138. *T.J. Hooper*, 60 F.2d at 739–40.

139. *Id.* at 740 (citations omitted).

140. CRITICAL INFORMATION, *supra* note 18, at 4.

141. 224 F.2d 120 (6th Cir. 1955).

142. *Id.* at 129. In a later case, a court declined to follow *Hooper* and *Northwest Airlines* because "[i]n neither case was the question of customary practice related to negligence in design," and "[c]arriers have traditionally been held to a higher standard of care than others." Ward v. Hobart Mfg. Co., 450 F.2d 1176, 1185 (5th Cir. 1971).

143. *See, e.g.*, Weirum v. RKO Gen., 539 P.2d 36, 40 (Cal. 1975) ("Liability is imposed only if the risk of harm resulting from the act is deemed unreasonable."); *see also* Deromedi v. Litton Indus. Prods., Inc., 636 F. Supp. 392, 395 (W.D. Mich. 1986) (finding that a

merely subjects him to liability."[144] In the area of secure software, no accepted tests currently exist for determining when a particular software vendor has breached its duty, although many have been proposed. For example, some scholars argue that software vendors should be found 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.'"[145]

D. Causation

Causation is established by a two-pronged test. First, the defendant's negligence must have been the cause-in-fact of the plaintiff's injury.[146] Cause-in-fact is proved by showing that "but for" the defendant's negligence, the injury would not have occurred,[147] or that the negligence was a "substantial factor" in bringing about the injury.[148]

In computer security breach cases, there are generally multiple factors involved in the breach. Not only must the software have certain security vulnerabilities, but a third party (generally a hacker or other cybercriminal) must intentionally exploit the vulnerabilities to gain access to the system. The user may also be partly at fault for not properly implementing available security measures. If the court applies a "but for" test, the software's security defects may be found not to be the cause-in-fact of damages, while if the court applies a "substantial factor" test, it is likely that the software defects will be held to be a substantial factor in the security breach.

Second, the defendant's conduct must have been the proximate (or legal) cause of the injury; that is, the plaintiff's damages must have been a foreseeable result of the defendant's negligent act.[149] For instance, in *Saloomey v. Jeppesen & Co.*,[150] the U.S. Court of Appeals for

---

breach of a statutory duty to provide a safe workplace did not supersede a worker's negligent use of equipment in determining the cause of an injury).

144. SECOND RESTATEMENT, *supra* note 111, § 4 cmt. a. In the *Second Restatement of Torts*, the term "subject to liability" is used "to denote the fact that the actor's conduct is such as to make him liable for another's injury, if (a) the actor's conduct is a legal cause thereof, and (b) the actor has no defense applicable to the particular claim." *Id.* § 5.

145. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1575 n.112 (2005).

146. DIAMOND ET AL., *supra* note 113, § 11.02, at 202.

147. *Id.*

148. *Id.* § 11.03, at 203.

149. *See, e.g.*, Evans v. Thomason, 72 Cal. App. 3d 978, 983 (1977) (explaining that "[t]he question is not whether [a] defendant did foresee, or by the exercise of ordinary care should have foreseen . . . [but] whether it is reasonably foreseeable that injury or damage would likely occur.").

150. 707 F.2d 671 (2d Cir. 1983).

the Second Circuit held that a navigational chart maker's use of erroneous information in its navigational maps was the proximate cause of a fatal airplane crash.[151] Unlike *Saloomey*, where damages arose from a specific, identifiable act of negligence, when a breach of security occurs, "it is often difficult to pinpoint just what has gone wrong."[152] Proving proximate cause becomes increasingly difficult as the software in question becomes longer and more complex—exactly the characteristics of most operating systems and other security-related software.

Foreseeability acts as a limitation both on a finding of causation[153] and on the amount and nature of damages that can be recovered for negligence.[154] As technology continues to develop, courts will likely find foreseeable activities that were less obvious (not foreseeable) in the past.[155]

E. Damages

A plaintiff is entitled to recover all damages proximately caused by a defendant's negligence.[156] These can include personal injuries,[157] property damage,[158] and, in some states, economic losses.[159] Punitive damages are not recoverable.[160]

It is not necessary for a defendant to anticipate every possible scenario under which someone could be injured. For example, "[i]t would be totally unreasonable to require that a manufacturer warn or protect against every injury which may ensue from mishap in the use

---

151. *Id.* at 677–78.

152. John M. Conley, *Tort Theories of Recovery Against Vendors of Defective Software*, 13 RUTGERS COMPUTER & TECH. L.J. 1, 16 (1987).

153. *See* DIAMOND ET AL., *supra* note 113, § 12.03, at 216.

154. *Id.*

155. Lawrence B. Levy & Suzanne Y. Bell, *Software Product Liability: Understanding and Minimizing the Risks*, 5 HIGH TECH. L.J. 1, 9–10 (1989); *see* Curtis E.A. Karnow, *Liability for Distributed Artificial Intelligence*, 11 BERKELEY TECH. L.J. 147, 180–81 (1996) (noting that what is reasonably foreseeable "depends on custom and what people generally believe. These in turn may depend on general impressions of what technology can do . . . . Reasonable foreseeability is a moving target; it dodges and weaves depending on public policy, and on the perceived technological sophistication of the population.").

156. *See supra* note 110 and accompanying text.

157. *See, e.g.*, Martin v. United States, 471 F. Supp. 6, 13 (D. Ariz. 1979) (permitting recovery for personal injuries, including past and future medical damages, loss of earning capacity, and pain and suffering).

158. *See, e.g.*, George A. Hormel & Co. v. Maez, 92 Cal. App. 3d 963, 966, 971 (1979) (affirming award covering damaged equipment in suit arising out of motor vehicle collision).

159. *See infra* Part II.F.2.

160. *See* Milwaukee & St. Paul Ry. v. Arms, 91 U.S. 489, 492–93 (1875) (recognizing that departure from the general prohibition on punitive damages is permissible only in cases of gross negligence).

of his product."[161] It is also not necessary for a plaintiff to show that the seller foresaw a specific injury or the amount of the loss. A plaintiff need only show that a reasonable person in the seller's position would have foreseen in the ordinary course of events that damages would follow from the seller's breach.[162]

The limitation placed on damage recovery by the foreseeability requirement can be extremely important in the computer context, where the hardware, and often the software, is specifically designed to be general-purpose.[163]

Where software is a mass-marketed operating system or security software, it is certainly foreseeable that it will be used in unmodified form to operate a computer system and secure that system against certain categories of harm, and that any defects in that software could lead to unauthorized intrusions into and damage to the system or the data stored in the system.[164]

F. Difficulties in Applying Negligence Law

1. Intervening and Superseding Causes

The issue of whether a computer system is insecure arises when someone has been able to obtain unauthorized access to the system through a vulnerability in software security. Such conduct is almost always criminal in nature. Under traditional negligence law, where damage is caused by a third party's criminal act, the potential liability

---

161. Borowicz v. Chicago Mastic Co., 367 F.2d 751, 760 (7th Cir. 1966); *see also* Perrine v. Pac. Gas & Elec. Co., 186 C.A.2d 442, 449 (1960) ("Even one who maintains so dangerous an instrumentality as a high power line need not anticipate at his peril every possible fortuitous circumstance under which someone may make contact with the wires causing injury . . . ."); *but see Hormel*, 92 Cal. App. 3d at 970 (holding the driver of a car who, while intoxicated, knocked down a utility pole, causing a power surge, liable for resulting damages to a nearby business).

162. Barnard v. Compugraphic Corp., 667 P.2d 117, 120 (Wash. Ct. App. 1983).

163. General-purpose computer systems may create problems because:

> [they] are designed to perform a variety of tasks, many of which may not have been envisioned by their creators. It may reasonably be argued that it is foreseeable that accounting software could cause certain damages to a business, such as lost revenues, lost profits, and even lost customers, if it were defective. It stretches credulity, however, to argue that it would be reasonably foreseeable to the developer of a word processing package that a defect in the package could cause billions of dollars in damages if used to develop an emergency procedure manual for a nuclear power plant.

David E. Jordan, *The Tortious Computer—When Does EDP Become Errant Data Processing?*, 4 COMPUTER L. SERV. § 5-1, art. 2, at 10 (1977).

164. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 274 (2005) (discussing that the *Palsgraf* rule is "equally applicable to cases involving database security").

of the negligent party generally is superseded by the criminal conduct unless it is determined to be "highly foreseeable."[165]

While security software vendors are certainly aware of hackers and others who have infiltrated computer systems by exploiting vulnerabilities in certain software packages,[166] that alone may not mean that the injury suffered by a particular plaintiff was highly foreseeable to the vendor. The proliferation of websites[167] and blogs[168] that report on security breaches in specific software packages, however, makes it at least arguable that a vendor knows or should know, not only of the flaws in its products, but also that injuries are likely to arise from a third party's exploitation of those breaches.

The duty analysis is also impacted by the fact that virtually all of the acts that result in damages from insecure computers are conducted by third parties who use the computer system to engage in criminal conduct. Courts have generally held that, except under extraordinary circumstances, a party is entitled to assume that third parties will not commit intentional criminal acts.[169]

---

165. Akins v. Dist. of Columbia, 526 A.2d 933, 935 (D.C. 1987). As stated in the *Restatement (Second) of Torts*:

> Whether he is liable or not depends on matters which are usually beyond his control. Thus, whether or not he is liable depends upon whether his breach of duty results in an injury to someone to whom the duty is owing in such a manner as to make the breach of the duty a legal cause of the injury, and this depends upon the course of events subsequent to the actor's breach of his duty, a matter over which the actor has no effective control . . . .

SECOND RESTATEMENT, *supra* note 111, § 4 cmt. a.

166. Software vulnerabilities are noted almost daily in the computer industry press and certain online sites. *See, e.g.*, *supra* notes 5–6; *see also* Rustad & Koenig, *supra* note 145, at 1570 ("In a networked world, it is reasonably foreseeable that computer hackers or cybercriminals will discover and exploit known vulnerabilities in operating systems.").

167. *See, e.g.*, Carnegie-Mellon Software Engineering Institute, CERT Coordination Center, http://www.cert.org (last visited Feb. 20, 2008) (reporting on business software security developments); SearchSecurity.com, http://searchsecurity.techtarget.com (last visited Feb. 20, 2008) (reporting "security-specific" news).

168. *See, e.g.*, London Software Testing News UK, http://testinglondon.wordpress.com (last visited Feb. 20, 2008) (blogging on international software testing news).

169. SECOND RESTATEMENT, *supra* note 111, § 302B cmt. d; *see also* Gaines-Tabb v. ICI Explosives USA, Inc., 995 F. Supp. 1304, 1318 (W.D. Okla. 1996) (holding that a manufacturer of fertilizer and blasting caps was not liable for bombing of a federal building because the manufacturer was entitled to believe that third parties would not engage in intentional criminal conduct). The reasons for this rule are twofold:

> The first reason is a probabilistic judgment that foreseeability analysis requires. Individuals generally are significantly deterred from undertaking intentional criminal conduct given the sanctions that can follow. The threatened sanctions make the third-party intentional criminal conduct sufficiently less likely that, under normal circumstances, we do not require the putative tort defendant to anticipate it . . . .

Does the distribution of insecure software involve the sort of extraordinary circumstances under which the software vendor should anticipate a third party's criminal act? There are two situations in which most courts have found extraordinary circumstances.

First, some courts have found extraordinary circumstances where the defendant has a "special relationship" with the victim and, thus, has a duty to protect the victim against third party intentional criminal conduct.[170] A vendor of security-related software generally does not have a special relationship with each licensee of its software. Typically, the only relationship is contractual, which does not alone create a special relationship for purposes of tort liability.[171] The contract defines the terms of the relationship, including the allocation of risks. Courts are traditionally unwilling to allow a party to a contract to avoid the limitations contained in the contract by bringing a negligence action.[172]

The second situation is where the defendant's affirmative actions "create a high degree of risk of [the third party's] intentional misconduct."[173]

> Generally, such circumstances are limited to cases in which the defendant has given a young child access to ultra-hazardous materials such as blasting caps or firearms. Even in those cases, courts have relied on the third party's severely dimin-

---

> The second reason is structural. The system of criminal liability has concentrated responsibility for an intentional criminal act in the primary actor, his accomplices, and his co-conspirators. By imposing liability on those who did not endeavor to accomplish the intentional criminal undertaking, tort liability would diminish the responsibility placed on the criminal defendant. The normative message of tort law in these situations would be that the defendant is not entirely responsible for his intentional criminal act.

James v. Meow Media, Inc., 300 F.3d 683, 694 (6th Cir. 2002).

170. *See, e.g.*, Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 358 (Cal. 1976) (noting that special relationships create an exception to the general rule that a person does not owe a duty to control the conduct of another).

171. *See, e.g.*, A.T. Kearney, Inc. v. IBM Corp., 73 F.3d 238, 240–42 (9th Cir. 1995) (finding no special relationship between the parties of a computer design contract); *see also* NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536, 1547 (N.D. Okla. 1997) (finding no duty beyond the contractual agreement, and, thus, denying tort remedies); Columbus McKinnon Corp. v. China Semiconductor Co., 867 F. Supp. 1173, 1179 (W.D.N.Y. 1994) (same).

172. In addition to direct purchasers, third parties injured by an insecure system (e.g., whose personal information is stolen from an insecure system or who are otherwise injured by a system malfunction) are even further removed from the vendor, and the two have no special relationship. *See, e.g.*, *James*, 300 F.3d at 693–94 (finding no special relationship between a video game developer and the victims of a video game player who was allegedly induced by the game to commit acts of violence).

173. SECOND RESTATEMENT, *supra* note 111, § 302B cmt. e.H.

> ished capacity to handle the ultra-hazardous materials. With older third parties, courts have found liability only where defendants have vested a particular person, under circumstances that made his nefarious plans clear, with the tools that he then quickly used to commit the criminal act.[174]

Neither of those circumstances arise in cases involving the distribution and use of insecure software. The licensee of the software is generally a sophisticated business entity or government agency with MIS staff who understand computers, software, and system security issues. These individuals are neither children nor those with "nefarious plans" to use the software to commit a criminal act.

However, in some states, courts have held that a duty may be found, even when third party criminal conduct is present, where "special circumstances" exist.[175]

A purveyor of insecure software should realize that its conduct may involve an unreasonable risk of harm to those who use or rely upon the software, and, therefore, it has a duty to exercise reasonable care to prevent that risk from occurring (i.e., a duty to provide secure software).[176]

2. Economic Loss Rule

Courts are split over whether economic losses are recoverable for negligence claims.[177] There are two aspects to the "economic loss"

---

174. *James*, 300 F.3d at 694–95 (citations omitted).

175. See Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1007 (N.H. 2003), in which the court recognized a "special circumstances" exception for when a party has created an unreasonable and foreseeable risk of criminal misconduct, and thus imposed a duty to prevent harm to those foreseeably endangered.

176. *See* Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 115, 130 (Mark F. Grady & Francesco Parisi eds., 2006) ("[K]ey infrastructure providers have been held liable even in the face of malicious acts by third parties who might naturally be understood to be the actual source of the harm.").

177. Some courts allow recovery for economic losses, at least in some circumstances. Interfase Mktg., Inc. v. Pioneer Techs. Group, Inc., 774 F. Supp. 1355, 1359–60 (M.D. Fla. 1991) (allowing a misrepresentation claim as an exception to the economic loss rule where no contract remedy was available); U.S. Welding, Inc. v. Burroughs Corp., 587 F. Supp. 49, 50 (D. Colo. 1984) (recognizing liability for pecuniary loss in a claim for negligent misrepresentation); J'aire Corp. v. Gregory, 598 P.2d 60, 64 (Cal. 1979) ("Recovery for injury to one's economic interests, where it is the foreseeable result of another's want of ordinary care, should not be foreclosed simply because it is the only injury that occurs."); Black, Jackson & Simmons, Ins. Brokerage, Inc. v. IBM Corp., 440 N.E.2d 282, 284 (Ill. App. Ct. 1982) (allowing recovery of economic losses for negligent misrepresentation).

Other courts have stated that economic losses are not recoverable. *See* Apollo Group, Inc. v. Avnet, Inc., 58 F.3d 477, 479–81 (9th Cir. 1995) (holding that the tort of negligent misrepresentation is not an exception to the economic loss rule, barring recovery strictly for pecuniary losses); Transp. Corp. of Am. v. IBM Corp., 30 F.3d 953, 956–57, 960 (8th

rule. The first is that a party to a contract for the sale of goods cannot recover under negligence law for economic losses that are unrelated to personal injury or property damages; recovery for such losses are to be determined by contract law.[178] This prohibition "is premised on the idea that such damages are recoverable under Uniform Commercial Code (U.C.C.) warranty provisions."[179] In other words, "there is no duty to exercise reasonable care to protect against a loss that is purely economic in nature."[180]

A typical case in which the economic loss rule has prevented recovery is where a computer failure resulted in only pecuniary damages, such as lost profits and lost goodwill.[181] While a licensee of insecure software may also suffer similar losses, security breaches may give rise to other, non-pecuniary losses—often of a much more severe nature.

For instance, a major security breach may cause the software user to suffer a significant loss of reputation, "an interest protected by tort law."[182] For example, in 2005, CardSystems Solutions suffered a security breach that exposed up to 40 million MasterCard accounts,[183] as well as credit card information from several other major credit card companies, to identity thieves.[184] The breach resulted in significant

---

Cir. 1994) (barring tort remedies to recover purely economic losses); Krider Pharmacy & Gifts v. Medi-Care Data Sys., Inc., 791 F. Supp. 221, 226 (E.D. Wis. 1992) (same); Wausau Paper Mills Co. v. Chas. T. Main, Inc., 789 F. Supp. 968, 971 (W.D. Wis. 1992) (same); Copiers Typewriters Calculators, Inc. v. Toshiba Corp., 576 F. Supp. 312, 325–26 (D. Md. 1983) (same); Jaskey Fin. & Leasing v. Display Data Corp., 564 F. Supp. 160, 166 (E.D. Pa. 1983) (same); Office Supply Co. v. Basic/Four Corp., 538 F. Supp. 776, 791–92 (E.D. Wis. 1982) (same); Affiliates for Evaluation & Therapy, Inc. v. Viasyn Corp., 500 So. 2d 688, 693 (Fla. Dist. Ct. App. 1987) (same).

178. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 470 (E.D. Va. 2002); *Office Supply Co.*, 538 F. Supp. at 791–92; Word Mgmt. Corp. v. AT&T Info. Sys., Inc., 525 N.Y.S.2d 433, 435 (N.Y. App. Div. 1988).

179. Rogers Merch., Inc. v. Bojangles' Corp., No. 87-C-5001, 1989 WL 6391, at *3 (N.D. Ill. Jan. 24, 1989). However, where the contract is deemed one for services, and not the sale of goods, U.C.C. Article 2 does not apply, and a suit for negligence would lie. *Word Mgmt. Corp.*, 525 N.Y.S.2d at 436.

180. Rockport Pharmacy, Inc. v. Digital Simplistics, Inc., 53 F.3d 195, 198 (8th Cir. 1995).

181. *See, e.g.*, *Krider Pharmacy*, 791 F. Supp. at 226 (rejecting a commercial purchaser's claim for damages based on lost earnings and lost reputation because a computer system did not cause damage to "other property").

182. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 21 cmt. c, illus. 1 (1998) [hereinafter THIRD RESTATEMENT].

183. Ashlee Vance, *MasterCard Fingers Partner in 40m Card Security Breach*, REGISTER, June 18, 2005, http://www.theregister.co.uk/2005/06/18/mastercard_breach.

184. It was claimed that the breach was due to vulnerabilities in Microsoft's Windows 2000 operating system and IIS Server 5.0. *See* Softpedia, Microsoft Software to Blame for the CardSystems Solutions Data Security Breach? (June 21, 2005), http://news.softpedia.

adverse publicity for CardSystems Solutions,[185] resulting in a major loss of reputation and several large customers, including VisaUSA and American Express.[186]

The second aspect of the "economic loss" rule is that where a product causes no personal injury or property damage (other than to the product itself), such damages are deemed economic loss for which no negligence claim lies.[187]

In *Transport Corp. of America v. IBM Corp.*,[188] for example, TCA sued IBM, claiming that a disk drive failure caused data to be damaged, resulting in lost income and data.[189] TCA asserted claims in negligence and strict liability.[190] The court barred TCA's recovery for lost data under the economic loss rule, holding that "where a defect in a component part damaged the product into which that component was incorporated, economic losses to the product as a whole [are] not losses to 'other property.'"[191] The court held that the data was in effect a component of the entire computer system and, thus, not separate property for tort law.[192]

Transport Corp. is clearly distinguishable from a situation where data is lost or destroyed due to insecure software. First, in the case of insecure software, the data is not lost or destroyed by the software itself, but by a third party who uses the vulnerabilities of the software to gain access to the computer system and uses that access to damage or destroy the data. The defect in the software leads only indirectly to

---

com/news/Microsoft-Software-to-Blame-for-the-CardSystems-Data-Security-Breach-3440.shtml. Those vulnerabilities allowed hackers to install rogue software to gain access to stored data. However, much of the blame was also laid at the feet of CardSystems itself, for failing to implement the agreed-upon security measures. Jonathan Krim & Michael Barbaro, *40 Million Credit Card Numbers Hacked*, WASH. POST, June 18, 2005, at A01.

185. *See, e.g.*, Jaikumar Vijayan & Todd Weiss, *CardSystems Breach Renews Focus on Data Security*, COMPUTERWORLD, June 20, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,1102646,00.html.

186. Bruce Schneier, Visa and AmEx Drop CardSystem (July 21, 2005), http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html.

187. *See* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 870–71 (1986) (explaining that purely economic loss is not recoverable in tort when "no person or other property" is damaged); *see also* Rockport Pharmacy, Inc. v. Digital Simplistics, Inc., 53 F.3d 195, 198 (8th Cir. 1995) (explaining that loss of data caused by a software problem is not damage to "other property").

188. 30 F.3d 953 (8th Cir. 1994).

189. *Id.* at 955–56.

190. *Id.* at 956.

191. *Id.* at 957 (citation omitted).

192. *Id.*; *accord Rockport Pharmacy*, 53 F.3d at 198 ("Rockport contends that it sustained a loss of data installed in the computer system. We conclude, however, that such losses represent nothing more than 'commercial loss for inadequate value and consequent loss of profits.'").

the loss or destruction of the data due to the intervention of a third party.

Second, unlike the complete computer system in *Transport Corp.*, where the data could be viewed as a component of the system itself, and where a vendor is providing only the software, any data entered into the computer system by the customer would not be considered part of the software—and hence not part of the "product."[193] The data and the software are separate forms of digital information. The data can be read and manipulated by the software, but it is created by the user or a third party, not the software vendor. Therefore, destruction of data due to insecure software should not be deemed damage to or destruction of the software itself, and should not bar recovery of damages by the licensee under the second prong of the economic loss rule.

3. Contractual Preclusion

A majority of courts hold that where a contract between a buyer and seller exists, a negligence claim is unavailable and the aggrieved party is limited to a breach of contract claim.[194] "The mere existence of a contract does not give rise to a duty in tort."[195] As stated by one court:

> In most circumstances, where a party to a transaction renders a service or sells a product, there would have been no duty to render that service or sell that product except for the voluntary undertaking to do so; that being true, the contract governing the transaction normally defines the scope of the parties' obligations to one another.[196]

---

193. *See, e.g.*, Saratoga Fishing Co. v. J.M. Martinac & Co., 520 U.S. 875, 879 (1997) (holding that items added to a product are "other property" and not part of the initial product). Thus, data input to the computer system by the software user should be considered "other property" and not part of the software "product."

194. *E.g.*, Mesa Bus. Equip., Inc. v. Ultimate S. Cal., Inc., No. 89-55825, 1991 WL 66272, at *4 (9th Cir. Apr. 30, 1991) (citing S.M. Wilson & Co. v. Smith Int'l, Inc., 587 F.2d 1363, 1376 (9th Cir. 1978)); Antel Oldsmobile-Cadillac, Inc. v. Sirus Leasing Co., 475 N.Y.S.2d 944, 945 (N.Y. App. Div. 1984) (noting that when an "injury is properly characterized" as economic loss, a "plaintiff is relegated to contractual remedies"); Westfield Chem. Co. v. Burroughs Corp., 21 U.C.C. Rep. Serv. 1293, 1299 (Mass. Super. 1977) ("The negligent manufacturing count fails since it is basically a duplicate of the warranty and contract counts and hence barred by the agreement . . . .").

195. *Rockport Pharmacy*, 53 F.3d at 198.

196. Heidtman Steel Prods., Inc. v. Compuware Corp., No. 3:97CV7389, 2000 WL 621144, at *12 (N.D. Ohio Feb. 15, 2000) (citing W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 92, at 657 (5th ed. 1984) [hereinafter PROSSER & KEETON]); *see also* Columbus McKinnon Corp. v. China Semiconductor Co., 867 F. Supp. 1173, 1183 (W.D.N.Y. 1994) ("[P]ublic policy does not warrant the imposition of a duty upon [a

Contractual limitations on liability will be enforced when ordinary negligence is involved, because "the U.C.C. should apply to commercial transactions where the product merely failed to live up to expectations and the damage did not result from a hazardous condition."[197]

Otherwise, if a court allowed the plaintiff to circumvent the negotiated allocation of risk provisions in a contract merely by dressing its claims in tort clothing, it "would interfere with the ability of the contracting parties to allocate and bargain for risk of loss. Warranty law, not tort law, protects the business purchaser's expectation of suitability and quality."[198]

The only exception to this rule is where the negligent conduct has caused physical damage to persons, property, or other tangible things (other than economic loss).[199]

III. APPLYING PRODUCT LIABILITY LAW TO INSECURE SOFTWARE

Under product liability law, liability is imposed on the theory that "[t]he costs of damaging events due to defectively dangerous products can best be borne by the enterprisers who make and sell these products."[200] For the plaintiff, there are many advantages to a product liability claim over a breach of contract claim. The two most important benefits are (i) no privity of contract is required for recovery, and (ii) contractual disclaimers and limitations are not enforceable.[201]

The *Restatement* (*Second*) *of Torts* Section 402A sets forth the elements of a claim for strict product liability:

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

---

computer design consultant] to exercise reasonable care beyond his contractual duties."); Richard A. Rosenblatt & Co. v. Davidge Data Sys. Corp., 743 N.Y.S.2d 471, 472 (N.Y. App. Div. 2002) (finding no "cognizable legal duty distinct from that created by the parties' contracts").

197. Transp. Corp. of Am. v. IBM Corp., 30 F.3d 953, 958 (8th Cir. 1994).

198. Kerry A. Kearney, *Computer Dissatisfaction: Should Tort Remedies Be Permitted or Does the U.C.C. Still Govern?*, 7 J.L. & COM. 243, 244–45 (1987).

199. *Heidtman Steel Prods.*, 2000 WL 621144, at *12.

200. PROSSER & KEETON, *supra* note 196, at 692–93; *see also* THIRD RESTATEMENT, *supra* note 182, § 2(b) (considering a product to have a defective design when the seller could have avoided foreseeable risks of harm by adopting a reasonably alternative design).

201. Neuburger & Garde, *supra* note 106, at 5.

> (a) the seller is engaged in the business of selling such a product, and
> (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.
> (2) The rule stated in Subsection (1) applies although
> (a) the seller has exercised all possible care in the preparation and sale of his product, and
> (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.[202]

The doctrine applies to "any product sold in the condition, or substantially the same condition, in which it is expected to reach the ultimate user or consumer."[203] Under Section 402A, the seller would be subject to strict liability "even though he has exercised all possible care in the preparation and sale of the product."[204]

> It is not a question of fault but simply a determination of how society wishes to assess certain costs that arise from the creation and distribution of products in a complex technological society in which the consumer thereof is unable to protect himself against certain product defects.[205]

However, the mere fact that a security device fails to protect the victim in a particular situation does not necessarily establish that the product was unreasonably dangerous.[206]

The *Restatement* (*Third*) *of Torts: Product Liability* reformulated product liability law by redefining *product defectiveness*:

> A product:
>
> (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product;

---

202. SECOND RESTATEMENT, *supra* note 111, § 402A.

203. *Id.* cmt. d.

204. *Id.* cmt. a.

205. Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1035 (9th Cir. 1991). However, the Ninth Circuit eventually refused to extend strict liability to the content of plaintiff's book. *Id.* at 1034–35.

206. *See, e.g.*, Elsroth v. Johnson & Johnson, 700 F. Supp. 151, 160–62 (S.D.N.Y. 1988) (holding the fact that a tamper-resistant seal could be defeated by a determined criminal did not make it unreasonably dangerous); Hampshire v. Ford Motor Co., 399 N.W.2d 36, 37–38 (Mich. Ct. App. 1986) (dismissing a lawsuit alleging an ignition locking system was defective because it was circumvented by a car thief); Aronson's Men's Stores, Inc. v. Potter Elec. Signal Co., 632 S.W.2d 472, 474 (Mo. 1982) (en banc) (holding that a malfunctioning burglary alarm system was not unreasonably dangerous).

> (b) is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe; . . . .[207]

Due care (negligence analysis) is explicitly excluded from this definition—it is a strict liability analysis.[208] It requires a determination of the "intended design" and a comparison of the intended design to the product itself. A design defect, on the other hand, arises from the failure to adopt a reasonable alternative design that would have made the product reasonably safe—a traditional negligence analysis.[209]

Accordingly, in applying product liability law to insecure software defects,[210] it is necessary to determine first whether the software insecurity is due to a design defect or a manufacturing defect.

Software development generally goes through a number of phases before reaching the user. These steps can be classified as (i) the design phase, (ii) the coding phase, (iii) the testing phase, and (iv) the replication and distribution phase.[211] There is no argument that a defect introduced into the product during the design phase would be deemed a design defect. And likewise there is no debate that a defect introduced into the product at the replication and distribution phase would be deemed a manufacturing defect. However, the most critical issue left open to debate is the coding phase (and to a lesser extent the testing phase). Should these phases be considered part of the design process or the manufacturing process of a software product?

Vendors would generally argue that everything before the replication and distribution phase is part of the product design process, hence, a negligence standard should apply to insecure software, except in the rare case where the defect occurred in the replication process.

---

207. THIRD RESTATEMENT, *supra* note 182, § 2.

208. *Id.* cmt. a.

209. *Id.*

210. No court decision has yet applied the *Third Restatement* to software defects. *See id.* § 19, Reporter's Notes to cmt. d. It has been argued that due to the *Third Restatement*'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." Rustad & Koenig, *supra* note 145, at 1577.

211. *See generally* MICHAEL D. SCOTT, 2 SCOTT ON INFORMATION TECHNOLOGY LAW § 10.04, at 10-6 (3d ed. 2007) (explaining the process of developing the specifications of software and websites).

VENDOR'S POSITION

Applicable Test	Software Development Phases
Design Defect/Negligence Standard	Design Phase Coding Phase Testing Phase
Manufacturing Defect/Strict Liability Standard	Replication and Distribution Phase

Licensees would argue that the design defect standard should apply only to defects introduced in the design phase, and that everything thereafter should be deemed part of the manufacturing phase—and subject to a strict liability standard.

LICENSEE'S POSITION

Applicable Test	Software Development Phases
Design Defect/Negligence Standard	Design Phase
Manufacturing Defect/Strict Liability Standard	Coding Phase Testing Phase Replication and Distribution Phase

The licensee's position is more in line with the commonly understood stages involved in software development[212]—that software design is generally completed before software coding begins.[213] The training and duties of software designers and coders are usually different, particularly among those working for the larger software vendors that are most likely to be developing operating systems and major security-related software products.[214]

---

212. *See* Peter A. Alces, *W(h)ither Warranty: The B(l)oom of Products Liability Theory in Cases of Deficient Software Design*, 87 CAL. L. REV. 269, 300 (1999) ("Here, the court need only conclude that the software failed because the program was actually *built* deficiently; that the *execution* of an admittedly reasonable software design was flawed.").

213. That does not mean that the design is necessarily set in stone when it gets to the programmers. Indeed, there is a feedback mechanism built into most software projects—if the programmers determine that there is a problem with the design, this information is conveyed to the designers and may result in changes made to the design document itself—which is then used by the coders to develop the software.

214. One court explained the job of a skilled programmer as a clerical function: "To a skilled programmer, the conversion of known input, known output, the mathematical expressions needed and the methods of transferring those expressions into computer language is necessarily a mere clerical function . . . . [T]he programmer, no matter how talented, does not express creativity, imagination, independent thought and uniqueness." Williams v. Arndt, 626 F. Supp. 571, 577–78 (D. Mass. 1985); *see also In re* Sherwood, 613

A. *Software as a "Product"*

Product liability law applies to "products." Is computer software a product or a service?[215] In the early, non-software case of *La Rossa v. Scientific Design Co.*, a court rejected a claim for strict liability for professional services on the grounds that

> [t]here is no mass production of goods or a large body of distant consumers whom it would be unfair to require to trace the article they used along the channels of trade to the original manufacturer and there to pinpoint an act of negligence remote from their knowledge and even from their ability to inquire.[216]

While the case did not directly address the software industry as it existed in 1968 (the year of the court's decision), the reasoning of the court for not applying strict liability to professional services mirrored the primitive state of the software industry at that time. There were no mass-marketed software products in 1968. Indeed, the personal computer market did not have its beginnings until the mid-1970s with the introduction of the Apple I and MITS Altair 8800.[217] In 1968, the computer industry was dominated by a handful of large mainframe computers located at government installations, universities, and large corporations.[218] Software was either custom made or heavily customized for each installation, and the customer dealt directly with the vendor, who generally provided the hardware, software, and all maintenance and support services. There was generally a direct, contractual relationship between the vendor and the customer. Thus, there was no need to extend product liability law to computer software.

Today, operating systems like Microsoft's Windows and security software like Symantec's Norton Firewall *are* mass produced and *are*

F.2d 809, 816–17 (C.C.P.A. 1980) (noting that writing a computer program can require a range of skills, from inventiveness to mere clerical skill).

215. Bruce Schneier supports the consideration of computer software as a product, stating: "Legislatures could impose liability on the computer industry, by forcing software manufacturers to live with the same product liability laws that affect other industries. If software manufacturers produced a defective product, they would be liable for damages." Schneier, *Liability*, *supra* note 50.

216. 402 F.2d 937, 942 (3d Cir. 1968).

217. *See* The MITS Altair 8800 and Apple I, http://www.csif.cs.ucdavis.edu/~csclub/museum/items/altair_8800_apple_1.html (last visited Feb. 20, 2008) (describing the two machines).

218. *See, e.g.*, Computer Sciences Corp., Our History, http://www.softwarehistory.org/history/d_60s.html (last visited Feb. 20, 2008).

distributed to a "large body of distant consumers."[219] These critical software packages are not custom crafted by a few individuals working in anonymity in their basement or garage. They are prepared by teams of hundreds of highly trained and skilled programmers who are carefully selected by their employers for their levels of expertise. Their programming is routinized, scrutinized, and supervised by experienced software development managers, who themselves are highly trained to perform their supervisory role.

In the almost four decades since the *La Rossa* decision, the software industry has evolved and matured to a point that, at least with regard to operating system and security software, it would not be unreasonable or unfair to hold software vendors responsible for defects to the same extent the courts hold other product designers responsible for defects in their products.[220] As noted in a recent government study: "Software code that is not well-designed from a security perspective is more likely than well-designed code to have weaknesses that could be exploited . . . . [C]ode can be designed so as to minimize such vulnerabilities, and well-developed procedures have been established to accomplish this goal."[221]

While a majority of courts have held that software is a *good*[222] for the application of the U.C.C.[223] and taxation,[224] that does not mean that software is necessarily a *product* for the application of product liability law.[225] Nor does the fact that a number of courts have held that

---

219. *Cf. supra* note 216 and accompanying text.

220. *See* Schneier, *Liability*, *supra* note 50 ("Today Firestone can produce a tire with a single systemic flaw and they're liable, but Microsoft can produce an operating system with multiple systemic flaws discovered per week and not be liable. This makes no sense, and it's the primary reason security is so bad today.").

221. CRS, *supra* note 17, at 15.

222. *See supra* Part III.C.

223. *See supra* note 70 and accompanying text.

224. *See, e.g.*, Comshare Inc. v. U.S., 27 F.3d 1142, 1149 (6th Cir. 1994) (holding that Comshare was entitled to the "tangible property" tax credit because "the intangible information on Comshare's master source code tapes and discs could not exist in usable form without the tangible medium").

225. James v. Meow Media, Inc., 90 F. Supp. 2d 798, 810 (W.D. Ky. 2000); *see* THIRD RESTATEMENT, *supra* note 182, § 19, Reporter's Notes to cmt. d (stating that courts "may draw an analogy between the treatment of software under the Uniform Commercial Code and under products liability law" when they must decide whether to apply strict liability to computer software, and explaining that "[u]nder the Code, software that is mass-marketed is considered a good. However, software that was developed specifically for the customer is a service.") (citations omitted). *But see* Hines v. JMJ Constr. Co., No. CV92-506329, 1993 WL 7269, at *4 (Conn. Super. Ct. Jan. 11, 1993) (adopting the U.C.C.'s definition of "goods" as the definition of "product").

software and data are "tangible property" for one purpose[226] mean that they are necessarily a "product" under product liability law. The *Third Restatement* provides that:

> [a] product is tangible personal property distributed commercially for use or consumption. Other items, such as real property and electricity, are products when the context of their distribution and use is sufficiently analogous to the distribution and use of tangible personal property that it is appropriate to apply the rules stated in this Restatement.[227]

The *Third Restatement* makes clear that the definition is not intended to be fixed, and "in every instance it is for the court to determine as a matter of law whether something is, or is not, a product."[228] Some states have modified the *Restatement* definition, arguably bringing software within the definition of a "product." For example, the Ohio statute defines a product as "any object, substance, mixture, or raw material that constitutes tangible personal property and that satisfies all of the following: (i) . . . capable of delivery itself . . . [;] (ii) . . . produced, manufactured, or supplied for introduction into trade or commerce . . . [; and] (iii) . . . intended for sale or lease to persons for commercial or personal use."[229] The issue in these situations will be whether computer software is "tangible personal property."

---

226. MW Mfrs., Inc. v. Friedman Corp., No. 97-C-8319, 1998 WL 417501, at *5 (N.D. Ill. July 21, 1998) (holding in tort action that software was tangible property because "[t]he end result that Plaintiff sought was a product (a software package) with certain identifiable capabilities"); *accord* Wal-Mart Stores, Inc. v. City of Mobile, 696 So. 2d 290, 291 (Ala. 1996) (holding that software was tangible personal property, the sale of which was subject to gross receipts tax); MAI Basic Four, Inc. v. Generic Bus. Solutions, Inc., CIV. A. No. 9908, 1990 WL 3665, at *2 (Del. Ch. Jan. 16, 1990) ("It is my view that documents or other physical objects containing confidential information, as well as computer disks or tapes containing software are tangible and thus able to be replevied."); S. Cent. Bell Tel. Co. v. Barthelemy, 643 So. 2d 1240, 1245 (La. 1994) ("[A]s computer software became more prevalent in society, and as courts' knowledge and understanding of computer software grew, later cases saw a shift in courts' attitudes towards the taxability of computer software, and courts began holding computer software to be tangible for sales, use and property tax purposes."); Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737–38 (Minn. Ct. App. 1991) (holding that computer tape and information contained on the tape were tangible property under a general liability provision limiting coverage to physical injury or destruction of tangible property).

227. THIRD RESTATEMENT, *supra* note 182, § 19(a).

228. *Id.* cmt. a.

229. OHIO REV. CODE ANN. § 2307.71(A)(12)(a) (LexisNexis 2005); *see also* TENN. CODE ANN. § 29-28-102(5) (2000) (defining a "product" as "any tangible object or goods produced"); Model Uniform Product Liability Act § 102(C), 44 Fed. Reg. 62714 (Oct. 31, 1979) (defining a "product" as "any object possessing intrinsic value, capable of delivery either as an assembled whole or as a component part or parts, and produced for introduction into trade or commerce").

In *America Online, Inc. v. St. Paul Mercury Insurance Co.*, AOL was sued by a group of disgruntled users who claimed that AOL 5.0 damaged their computer systems.[230] AOL brought suit against its insurer to force it to defend AOL under their insurance policy.[231] The insurance policy required St. Paul to cover and defend AOL in claims for "property damage," defined as "physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged."[232]

The complaint alleged that AOL 5.0 "damaged [consumers'] software, damaged their data, damaged their computers' operating systems, and caused the loss of data and the loss of use of the computers."[233] AOL contended that computer data, software, and system were tangible property, because they are "capable of being realized."[234] St. Paul argued that computer data and the like are not tangible property because "they constitute property that one cannot touch."[235] The court agreed with the insurance company, holding that "the plain and ordinary meaning of the word tangible is something that is capable of being touched or perceptible to the senses. Computer data, software, and systems do not have or possess physical form and are therefore not tangible property as understood by the Policy."[236]

However, in *Retail Systems, Inc. v. CNA Insurance Cos.*,[237] a Minnesota state court reached the opposite result. In that case, a computer consultant filed a declaratory judgment action against its insurer seeking a declaration that its general liability policy provided coverage for the loss of a client's computer tape and data and that the insurer was required to defend him against the client's action for damages.[238] Finding that the data constituted tangible personal property, the court said: "The data on the tape was of permanent value and was integrated completely with the physical property of the tape. Like a motion picture, where the information and the celluloid medium are

230. 207 F. Supp. 2d 459, 461 (E.D. Va. 2002).

231. *Id.*

232. *Id.* at 462–63 (citation and internal quotation marks omitted).

233. *Id.* at 466.

234. *Id.*

235. *Id.*

236. *Id.* at 467; *accord* State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) ("[C]omputer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.").

237. 469 N.W.2d 735 (Minn. Ct. App. 1991).

238. *Id.* at 736–37.

integrated, so too were the tape and data integrated at the moment the tape was lost."[239]

In a series of cases, courts have held that certain types of information will be deemed products, and that product liability law will apply to errors in such information.[240] In *Saloomey v. Jeppesen & Co.*,[241] inaccuracies in the information used to create aeronautical charts caused a fatal airplane crash.[242] The court held that because the charts were mass-produced and because purchasers substantially relied upon them without making alterations to them, the information was a product for strict liability purposes.[243] The court held that the publisher had a "special responsibility, as seller, to insure that consumers will not be injured by the use of the charts . . . . This special responsibility lies upon Jeppesen in its role as designer, seller and manufacturer."[244]

In *Fluor Corp. v. Jeppesen & Co.*,[245] a California state court was faced with the same issue. Reversing a trial court ruling that the defendant's charts were not products, the appellate court said:

> [The trial court] explained that it believed strict liability principles are applicable only to items whose physical properties render them innately dangerous, e.g., mechanical devices, explosives, combustible or flammable materials, etc. This belief was erroneous . . . . [A]lthough 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.[246]

---

239. *Id.* at 737.

240. As stated in the *Third Restatement*: "One area in which some courts have imposed strict products liability involves false information contained in maps and navigational charts. In that context the falsity of the factual information is unambiguous and more akin to a classic product defect." THIRD RESTATEMENT, *supra* note 182, § 19 cmt. d.

241. 707 F.2d 671 (2d Cir. 1983).

242. *Id.* at 672–73.

243. *Id.* at 676–77. "Though a 'product' may not include mere provision of architectural design plans or any similar form of data supplied under individually tailored service arrangements, the mass production and marketing of these charts requires Jeppesen to bear the costs of accidents that are proximately caused by defects in the charts." *Id.* at 677 (citation omitted).

244. *Id.* at 677; *see also* Aetna Cas. & Sur. Co. v. Jeppesen & Co., 642 F.2d 339, 341–43 (9th Cir. 1981) (assuming that the Federal Aviation Administration's flight data contained on the charts was a "product" for strict liability purposes).

245. 216 Cal. Rptr. 68 (Cal. Ct. App. 1985).

246. *Id.* at 71–72 (citations omitted).

The fact that a product requires "some professional skill" does not preclude the application of strict product liability.[247] "If suitable for mass marketing, the information is in some sense a fungible good for which the manufacturer placing it on the market must assume responsibility."[248] "Jeppesen mass produced and distributed thousands of charts on the aviation market. Implicit in their presence on the market was the representation that the purchaser could rely on their information safely. Exposing defendant Jeppesen's conduct to strict products liability is thus entirely appropriate."[249]

Citing the various *Jeppesen* decisions finding a publisher liable for erroneous data incorporated into its aeronautical charts, the United States Court of Appeals for the Ninth Circuit in *Winter v. G.P. Putnam's Sons*, held that those cases did not stand for the proposition that ideas and expressions alone were "products."[250] Instead, the court distinguished the characterization of the aeronautical charts as products for strict liability purposes, stating that "[a]eronautical charts are highly technical tools. They are graphic depictions of technical, mechanical data."[251] The court then continued, admittedly in *dictum*, to state: "Computer software that fails to yield the result for which it was designed may be another"[252]—that is, may be a product for strict liability purposes. The court in *Winter* further surmised that:

> [U]nder products liability law, the injury does not have to be caused by impact from the physical properties of the item. In other words, the injury does not have to result because a compass explodes in your hand, but can result because the compass malfunctions and leads you over a cliff.[253]

Where the definition of "product" does not provide an unequivocal answer in a particular case, the *Third Restatement* indicates that the determination[254] should be reached

---

247. Halstead v. U.S., 535 F. Supp. 782, 791 (D. Conn. 1982). This case involved the same aeronautical charts that were at issue in *Jeppesen*. *Id.* at 784–85.

248. *Id.* at 791.

249. *Id.*; *accord* Brocklesby v. U.S., 767 F.2d 1288, 1294–96 (9th Cir. 1985) (holding that a graphic instrument approach chart was a "product" subject to strict liability law).

250. Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1036 (9th Cir. 1991).

251. *Id.*

252. *Id.*

253. *Id.* at 1036 n.4. The Reporter's Notes of the *Third Restatement of Torts* note that *Winter* is a leading case in the field. *See* THIRD RESTATEMENT, *supra* note 182, § 19, Reporter's Notes to cmt. d.

254. Determining whether something is a "product" is an issue of law for the court to decide. *E.g.*, Johnson v. Murph Metals, Inc., 562 F. Supp. 246, 249 (N.D. Tex. 1983); *see also* THIRD RESTATEMENT, *supra* note 182, § 19, Reporter's Notes to cmt. d.

> in light of the public policies behind the imposition of strict liability in tort. Some of the policy considerations include: (1) the public interest in life and health; (2) the invitations and solicitations of the manufacturer to purchase the product; (3) the justice of imposing the loss on the manufacturer who created the risk and reaped the profit; (4) the superior ability of the commercial enterprise to distribute the risk of injury as a cost of doing business; (5) the disparity in position and bargaining power that forces the consumer to depend entirely on the manufacturer; (6) the difficulty in requiring the injured party to trace back along the channel of trade to the source of the defect in order to prove negligence; and (7) whether the product is in the stream of commerce.[255]

While these factors may not argue in favor of finding all software to be products, they strongly favor finding software that is supposed to provide security for corporate and government computer systems to be a product for product liability purposes.

B. Insecure Software as a Design Defect

Under the *Third Restatement*, a negligence standard is to be applied in design defect claims. The *Third Restatement* adopts the "risk-utility" analysis as the sole test for determining design defectiveness.[256] This test is based on the Learned Hand formula (B < PL) set forth in *United States v. Carroll Towing Co.*[257] Under that formula, the court will look at the burden (cost) to the vendor of making its product less defective, and balance that burden against the probability of injury to the user from using that defective product multiplied by the magnitude of the injury that the user may suffer as a result of the defect.[258]

It does not take an expert to understand that defects in software can and often do lead to massive damages to software users and third parties as a result of hackers, system crashes, and other manifestations of those defects.[259] This is particularly true in the area of system security, where the potential injury may be incalculable. How do you put a price tag on the damage caused by a hacker shutting down an

---

255. THIRD RESTATEMENT, *supra* note 182, § 19, Reporter's Notes to cmt. a.

256. *Id.* § 2(b) & cmt. d.

257. 159 F.2d 169, 173 (2d Cir. 1947).

258. *See id.* Some argue that "[t]he technical burden involved with security evaluations of complex systems weighs in favor of [software vendors] bearing the brunt of implementing security in product design." Kenneally, *supra* note 51, at 67.

259. It was reported that in a single month, October 2003, hackers caused over $1 billion in damages to computer systems. *See* Tim Lemke, *Spam Harmed Economy More Than Hackers, Viruses, Report Shows*, WASH. TIMES, Nov. 10, 2003.

air traffic control system during a blizzard, or a terrorist causing a water treatment plant to over-chlorinate the drinking supply of a major city and poisoning its citizens? These doomsday scenarios (and countless others) are all too real when you consider how much companies, government agencies, and individuals rely on software-controlled devices to protect and assist them in their daily duties.[260]

With regard to a product's *design*, negligence law requires a manufacturer to "exercise reasonable care in a variety of different functions."[261] With security-related software, the vendor's responsibilities would include carefully formulating the design of the software to prevent vulnerabilities that can be exploited by hackers and other third parties, properly implementing the design in code, thoroughly testing the code to expose any vulnerabilities, and revising the code to remove the vulnerabilities before releasing the software to the public.[262]

Under the *Third Restatement*, the analysis focuses on whether there was a "reasonable alternative design" available.[263] It does not require the vendor to rid its software of every vulnerability. Whether a "reasonable alternative design" for any given operating system or security application is available is a fact-specific inquiry and will differ for each software product at issue. But experience has shown that what is often needed for software containing security-related flaws is not an extensive redesign of the entire software package, but merely the rewriting of a small portion of the code to remove the vulnerability.

C. Insecure Software as a Manufacturing Defect

Under the *Third Restatement*, strict liability continues to apply to cases involving manufacturing defects. Manufacturers are "obliged to keep abreast of any scientific discoveries and are presumed to know the results of all such advances."[264] Further, they "bear the duty to

---

260. *See generally* CRITICAL INFORMATION, *supra* note 18.

261. OWEN, *supra* note 110, § 2.1, at 62. These functions include:

> that the general product concept be conceived and formulated carefully for its foreseeable uses and abuses; that proper attention be devoted to selecting appropriate materials and components to be assembled together into the finished product; that safety devices for the product's expected uses be adopted as appropriate; and that prototypes of the product be tested, as appropriate, in contexts duplicating the harshest circumstances of expected use.

Id.

262. "[A] study by Andrew Jacquith found that seventy percent of security weaknesses resulted from design flaws that could have been anticipated by a greater emphasis on security." Skibell, *supra* note 49, at 112.

263. *See supra* notes 207–209 and accompanying text.

264. Dartez v. Fibreboard Corp., 765 F.2d 456, 461 (5th Cir. 1985).

fully test their products to uncover all scientifically discoverable dangers before the products are sold."[265]

Those supporting the application of strict liability to defective software argue that the vendor should be held liable because (i) the vendor is in the best position to prevent software vulnerabilities; (ii) the vendor will be motivated to develop secure software; (iii) the vendor can spread the cost of providing secure software by increasing the price of its products; and (iv) the vendor will "treat the burden of . . . injury as a cost of production to be covered by liability insurance."[266]

Over the last twenty years, there have been calls to impose strict product liability on software vendors for defects in their products,[267] but to no avail. To date, there are no reported decisions in the United States holding a software vendor liable under a strict liability theory.

Opponents of strict liability for software vulnerabilities argue that the spectre of potentially massive damage awards would inhibit innovation and cause vendors to avoid developing products in these areas.[268] They also point out that the user of their software is in a better position to evaluate the risks it faces if there is a business interruption—whether due to software vulnerabilities or other causes—and to insure against such eventualities.[269] Vendors also point out that in complex software products defects are inevitable[270] and cannot be

---

265. *Id.*

266. Saloomey v. Jeppesen & Co., 707 F.2d 671, 677 (2d Cir. 1983).

267. *See, e.g.*, Patrick E. Bradley & Jennifer R. Smith, *Liability Issues Regarding Defects in Software*, 19 PRODUCT LIABILITY L. & STRATEGY, Nov. 2000, at 5, 5; Michael R. Maule, *Applying Strict Products Liability to Computer Software*, 27 TULSA L.J. 735, 737 (1992) (arguing that strict products liability of computer software manufacturers is desirable); Lori A. Weber, Note, *Bad Bytes: The Application of Strict Products Liability to Computer Software*, 66 ST. JOHN'S L. REV. 469, 471 (1992) (advocating for a fact-specific inquiry for determining whether to apply strict liability in computer software cases). *Contra* 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, 122–23 (1992) (concluding that strict liability can, but should not, be applied against computer software manufacturers).

268. *See* Steve Lohr, *Product Liability Lawsuits Are New Threat to Microsoft*, N.Y. TIMES, Oct. 6, 2003, at C2 (reporting that software executives believe that the imposition of product liability lawsuits "would chill innovations and undermine the competitiveness of American companies").

269. *See* Statement of Robert Holleyman, President and CEO of the Business Software Alliance Before the House of Representatives Committee on Science, *reprinted at* http://www.house.gov/science/holleyman_09-24.htm (last visited Feb. 20, 2008).

270. *See, e.g.*, Skibell, *supra* note 49, at 110.

prevented even by using today's software development "best practices."[271]

The issue of whether the vendor, for any given software package, should be held strictly liable for a manufacturing defect should not depend on generalized public policy arguments, but instead should result from an analysis of the vendor's coding and testing methodologies and whether they comport with the general legal rules applicable to product liability law.

D. Difficulties in Applying Product Liability Law

1. Economic Loss Rule

The most significant impediment to the use of strict product liability law to recover damages caused by insecure software is the "economic loss rule [which] generally bars claims in tort for economic losses, limiting recovery for such losses to the law of contract."[272] The *Third Restatement* defines economic losses[273] and indicates that because "products liability law lies at the boundary between tort and contract," some forms of loss, including pure economic loss, "are more appropriately assigned to contract law and the remedies set forth in Articles 2 and 2A of the Uniform Commercial Code."[274]

In most cases involving defective software, typical losses suffered by a plaintiff will involve the loss or corruption of data, lost employee time, or the cost of remediation.[275] Traditionally, "[s]uch losses fall within the economic loss doctrine and cannot be recovered in a prod-

---

271. *See* Lohr, *supra* note 268; Michael C. Gemignani, *Product Liability and Software*, 8 RUTGERS COMPUTER & TECH. L.J. 173, 191 (1981) ("[T]esting . . . can never prove the absence of fatal flaws in software. Testing can at best establish that the program is not likely to fail under certain uses.").

272. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 470 (E.D. Va. 2002); *see also* Word Mgmt. Corp. v. AT&T Info. Sys., Inc., 525 N.Y.S.2d 433, 435–36 (N.Y. App. Div. 1988) (concluding that if a transaction is deemed to be a sale of goods and the recovery sought is purely economic relief, the U.C.C. applies rather than negligence or strict products liability). For a discussion of the economic loss rule as it applies to negligence claims, see *infra* Part II.F.2.

273. The *Third Restatement* states:

> harm to persons or property includes economic loss if caused by harm to:
>
> (a) the plaintiff's person; or
>
> (b) the person of another when harm to the other interferes with an interest of the plaintiff protected by tort law; or
>
> (c) the plaintiff's property other than the defective product itself.

THIRD RESTATEMENT, *supra* note 182, § 21.

274. *Id.* cmt. a.

275. Neuburger & Garde, *supra* note 106, at 11.

uct liability action"[276] because they "stem from the alleged failure of the computer system to perform as expected and not from injury to another person or property."[277]

Arguments can be made, however, that some claims arising from the failure of security software should be recoverable despite the economic loss rule.[278] For example, a company's reputation "is an interest protected by tort law . . . ."[279] Additionally, the data contained in the computer is property separate and apart from the software itself.

2. *Contractual Disclaimers and Limitations on Liability*

Courts have held that the U.C.C. generally is intended to displace tort liability with regard to property damages, at least in the commercial context.[280] This rule remains a significant impediment to the application of product liability law in the security software context.

IV. APPLYING PROFESSIONAL MALPRACTICE LAW TO INSECURE SOFTWARE

Under the doctrine of professional malpractice, one who is deemed a *professional* will owe the other party a duty to act not just as a reasonable person under the circumstances, as required by negligence law, but to meet a higher standard—that of a professional in that particular field.[281] The concept of professional liability has generally been applied to those who by virtue of specific training and licensing are deemed to have a level of skills higher than that of nonprofessionals.[282]

---

276. *Id.*; *see also* Affiliates for Evaluation & Therapy, Inc. v. Viasyn Corp., 500 S.2d 688, 693 (Fla. Dist. Ct. App. 1987) (holding that because plaintiff suffered solely economic losses from a malfunctioning computer, a products liability action could not stand).

277. Krider Pharmacy & Gifts, Inc. v. Medi-Care Data Sys., Inc., 791 F. Supp. 221, 226 (E.D. Wis. 1992); *see also* Fishbein v. Corel Corp., No. 230-1995, 1996 WL 895317, at *4–5 (Pa. Com. Pl. Mar. 12, 1996).

278. *See, e.g.*, Spagnol Enters., Inc. v. Digital Equip. Corp., 568 A.2d 948, 951–52 (Pa. Super. Ct. 1989) (holding that warranty claims may apply even when loss from a product defect is purely economic).

279. *See* THIRD RESTATEMENT, *supra* note 182, § 21 cmt. c, illus. 1 (stating that an individual professional reputation is an interest protected by tort law).

280. *See, e.g.*, Transp. Corp. of Am., Inc. v. IBM Corp., 30 F.3d 953, 956 (8th Cir. 1994) (noting that the economic loss doctrine "bars recovery under the tort theories of negligence or strict liability for economic losses . . . ."); *see also infra* Part II.F.3.

281. *See supra* note 123 and accompanying text.

282. *Id.* Those persons falling within the realm of professional responsibility include doctors, lawyers, dentists, architects, accountants, and similarly licensed workers. *See* STUART M. SPEISER ET AL., 4 THE AMERICAN LAW OF TORTS 303–06 (1987) (enumerating the professions where malpractice liability has been imposed).

To date, courts have been reluctant to hold computer designers or programmers to the higher standard of professionals due to the lack of "established educational standards or regulations governing the performance of software programmers and developers, and [because] they are not licensed as professionals."[283] Early cases declined to create a tort "premised upon a theory of elevated responsibility on the part of those who render computer sales and services."[284] In *Hospital Computer Systems, Inc. v. Staten Island Hospital*, for example, the court refused to hold a computer programmer to a professional standard because:

> A profession is not a business. It is distinguished by the requirements of extensive formal training and learning, admission to practice by a qualifying licensure, a code of ethics imposing standards qualitatively and extensively beyond those that prevail or are tolerated in the marketplace, a system for discipline of its members for violation of the code of ethics, a duty to subordinate financial reward to social responsibility, and, notably, an obligation on its members, even in non-professional matters, to conduct themselves as members of a learned, disciplined, and honorable occupation.[285]

Other courts have refused to recognize computer programmers and consultants as professionals, because "[t]o lift the theory of malpractice from its narrow origin of personal, professional services to a lay patient or client and apply it to the law of commercial contracts would obfuscate the necessary boundaries of these two areas of law."[286]

The early cases were based on the fact that the software industry was in its infancy, and

---

283. Levy & Bell, *supra* note 155, at 10.

284. Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 479 F. Supp. 738, 740–41 n.1 (D.N.J. 1979), *aff'd in part, remanded in part on other grounds*, 635 F.2d 1081 (3d Cir. 1980) ("Simply because an activity is technically complex and important to the business community does not mean that greater potential liability must attach."); *see also* Triangle Underwriters, Inc. v. Honeywell, Inc., 604 F.2d 737, 745–46 (2d Cir. 1979) (declining to consider sellers or manufacturers of computer machinery as "members of the learned professions"); Atkins Nutritionals, Inc. v. Ernst & Young, LLP, 754 N.Y.S.2d 320, 322 (N.Y. App. Div. 2003) (refusing to recognize claim of professional malpractice by computer consultants); Richard A. Rosenblatt & Co. v. Davidge Data Sys. Corp., 743 N.Y.S.2d 471, 472 (N.Y. App. Div. 2002) (same).

285. Hosp. Computer Sys., Inc. v. Staten Island Hosp., 788 F. Supp. 1351, 1361 (D.N.J. 1992); *see also* Rogers Merch., Inc. v. Bojangles' Corp., No. 87-C-5001, 1989 WL 6391, at *3 (N.D. Ill. Jan. 24, 1989) (holding that tort liability does not attach to every activity whose practitioners call themselves professionals).

286. Columbus McKinnon Corp. v. China Semiconductor Co., 867 F. Supp. 1173, 1182–83 (W.D.N.Y. 1994).

1. Software was generally custom-developed for individual clients and not mass-produced;

2. Software vendors were small, cottage-type operations and not major corporations;

3. Software development was more of an art than a science; there was little in the way of organized education for developers and there were no standardized methods for developing software;

4. All software had "bugs" and there was no effective means of preventing bugs; and

5. Computers were useful, but not indispensable, tools for businesses.

Advances in software development methodology, education and standards, the emergence of major software corporations (such as Microsoft), and the required use of software in critical applications (e.g., network security, medical technology, nuclear reactor controls, weapon systems) have changed the landscape to the point that it may be time to rethink the logic behind these earlier cases and to establish a framework within which software vendors could be held liable as professionals for distributing insecure software.

Many software developers, particularly those at companies developing secure software, have received extensive training in the use of certain programming and testing techniques.[287] They have had to pass rigorous tests to become "certified."[288] In doing so, the certifying organization has established that these programmers have reached a level of expertise not held by general programmers. While this is not identical to the licensing requirements of state licensing boards such as state bar associations or medical boards, it may be sufficient to justify holding these certified developers to a higher, professional standard, particularly where their certifications relate to secure software development.

---

287. Today, a majority of colleges and universities have their Computer Science degrees accredited by the Computer Sciences Accreditation Commission (CSAS)/Computing Sciences Accreditation Board (CSAB). Computing Sciences Accreditation Board, http://www.csab.org (last visited Feb. 20, 2008); Accreditation Board of Engineering and Technology (ABET), http://www.abet.org (last visited Feb. 20, 2008).

288. For example, the International Information Systems Security Certification Consortium promotes the Certification for Information System Security Professional (CISSP) certification examination. CISSP.com, http://cissp.com (last visited Feb. 20, 2008); *see also* Patricia Haney DiRuggiero, Note, *The Professionalism of Computer Practitioners: A Case for Certification*, 25 SUFFOLK U.L. REV. 1139, 1151, 1151 n.63, 1161 (1991) (advocating certification of computer programmers and suggesting that the certificate program of the Institute for Certification of Computer Professionals (ICCP) provides a logical model).

In *Diversified Graphics, Ltd. v. Groves*, for example, the plaintiff hired a large accounting firm to help it locate a turnkey computer system.[289] When the chosen system proved inadequate for the company's needs, the company sued.[290] The court ruled that the accounting firm should be held to the American Institute of Certified Public Accountants' Management Advisory Service Practice Standards, which the firm had incorporated into its guidelines for internal use.[291] While the court refused to acknowledge a cause of action for computer malpractice, by holding the accounting firm to the AICPA standards, it achieved essentially the same result.

In *Data Processing Services, Inc. v. L.H. Smith Oil Corp.*, the plaintiff claimed that the defendant was negligent in designing an accounting and data processing software system.[292] The state appellate court stated in *dictum* that "[t]hose who hold themselves out to the world as possessing skill and qualifications in their respective trades or professions impliedly represent they possess the skill and will exhibit the diligence ordinarily possessed by well informed members of the trade or profession."[293] The court concluded that "[t]he situation here is more analogous to a client seeking a lawyer's advice or a patient seeking medical treatment for a particular ailment than it is to a customer buying seed corn, soap, or cam shafts."[294]

While there is a wide range of experience and expertise exhibited by computer software designers and programmers, those who develop operating systems and security software are generally at the higher end of the profession in terms of education, training, and experience. Although it is unlikely that a single, professional standard can or should be deemed to exist for those who design or write all types of software—from the mundane to the sublime—it is certainly possible to hold programmers who write critical software, such as operating systems and security software, to a higher standard than those who write less critical code such as word processors and videogames.

One problem with attempting to apply malpractice principles to software developers is the fact that most software today is developed by teams, often consisting of hundreds of people, and not just a single professional. These teams include software analysts, programmers,

---

289. 868 F.2d 293, 294–95 (8th Cir. 1989).

290. *Id.* at 295.

291. *Id.* at 296–97.

292. Data Processing Servs., Inc. v. L.H. Smith Oil Corp., 492 N.E.2d 314, 316 (Ind. Ct. App. 1986).

293. *Id.* at 319.

294. *Id.*

project managers, quality assurance engineers, technical writers, test engineers, and more. While many of these people may have the educational training and certifications indicative of a professional, others will not. How does a plaintiff establish that the defects in the software were due to the malpractice of the "professionals" who worked on the product and not those who would be deemed non-professionals?[295]

Another impediment to the application of malpractice to software development is the fact that "when an action for malpractice is product-oriented, a plaintiff cannot sue the professional in tort."[296] To the extent that the software is considered a product, malpractice principles will not apply.

V. THE SARBANES-OXLEY ACT AND ITS POTENTIAL IMPACT ON VENDOR LIABILITY

In the end, a primary goal of SOX will be more secured networks . . . .[297]

The Sarbanes-Oxley Act[298] (SOX) was enacted to ensure the accuracy of, and restore investor confidence in, the financial statements provided by corporations to government regulators, such as the Securities and Exchange Commission (SEC).[299] It was enacted in response to several high-profile accounting scandals involving Enron, Worldcom (MCI), Global Crossings, and Tyco International that resulted in billions of dollars in corporate and investor losses.[300]

SOX applies to both U.S. publicly owned corporations (and their wholly owned subsidiaries) and all foreign publicly owned corporations whose shares are registered with the SEC.[301] The SEC enforces

---

295. For example, in *Pezzillo v. General Telephone & Electronics Information Systems., Inc.*, 414 F. Supp. 1257, 1264–66, 1268–70 (M.D. Tenn. 1976), *aff'd per curiam*, 572 F.2d 1189 (6th Cir. 1978), the court held that computer programmers are not employed in a professional capacity as that term is used in the Fair Labor Standards Act of 1938. The court analogized the duties performed by computer programmers to those of a draftsman employed by an architect, stating that both the draftsman and the programmer generally performed mechanical functions, while architects and computer analysts generally acted as professionals. *Id.* at 1264–65.

296. Analysts Int'l Corp. v. Recycled Paper Prods., Inc., No. 85-C-8637, 1987 WL 12917, at *6 (N.D. Ill. June 19, 1987) (citing Kishwaukee Cmty. Servs. Ctr. v. Hosp. Bldg. & Equip. Co., 638 F. Supp. 1492, 1504 (N.D. Ill. 1986)).

297. Anne Saita, *Sarbanes-Oxley Act: You Ready Yet?*, SEARCHSECURITY.COM, Oct. 6, 2004, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1012386,00.html.

298. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified in Titles 11, 15, 18, 28, 29 of the U.S.C.).

299. *See supra* notes 25–27 and accompanying text.

300. *Id.*

301. 15 U.S.C. § 7201(7) (Supp. IV 2006); Saita, *supra* note 297.

the Act.[302] The Act requires that CEOs and CFOs certify that reports periodically filed with the SEC fairly present the company's financial condition.[303]

SOX does not specify the processes or systems a public company must undertake to comply with the Act. In general, the company needs to install multiple security technologies, including firewalls, intrusion detection systems, anti-virus software, and so forth.[304] But more is required. SOX "is subject to such broad interpretation as to make its implementation and enforcement in the IT world a nightmare."[305]

Pursuant to the Act, the SEC created the Public Company Accounting Oversight Board (PCAOB)[306] to oversee public company auditors, protect investors, and insure that auditors conduct informative, fair, and independent audits.[307] The PCAOB was given the task of developing corporate compliance requirements.[308] It developed and issued its Proposed Accounting Standards,[309] which provide additional guidance for assessing compliance with SOX.[310]

The Act has many sections, but those that most directly impact software and system security issues are Section 302 (making corporate officers and directors personally liable for misreporting financial information)[311] and Section 404 (requiring corporate officers, directors, and independent auditors to attest annually to the accuracy of the internal financial controls).[312]

---

302. 15 U.S.C. § 7202.

303. *Id.* § 7241.

304. *See* John De Santis, *Why Network Security Should Go Further Than Sarbanes-Oxley*, COMPUTERWORLD, Dec. 4, 2003, http://www.computerworld.com/securitytopics/security/story/0,10801,87704.00.html (discussing the requirements of SOX and its implications for computer companies).

305. *Id.*

306. 15 U.S.C. § 7211(a). For further information on the PCAOB, see The Public Company Accounting Oversight Board, http://www.pcaobus.org (last visited Feb. 20, 2008).

307. 15 U.S.C. § 7211(a).

308. *Id.* § 7211(c).

309. Press Release, PCAOB, Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements (Mar. 9, 2004), *available at* http://www.pcaobus.org/rules/docket_008/2004-03-09_release_2004-001-all.pdf [hereinafter PCAOB Release No. 2004-001].

310. The Audit Standard "establishes requirements and provides directions that apply when an auditor is engaged to audit both a company's financial statements and management's assessment of the effectiveness of internal controls over financial reporting." *Id.* at A-5.

311. 15 U.S.C. § 7241.

312. *Id.* § 7262.

The cost of compliance with the Act is enormous. It is estimated that U.S. public companies spent about $5.5 billion in 2004 to comply with the Act, and an additional $5.8 billion in 2005.[313]

A. Section 302

Section 302 of the Act states that the CEO and CFO are directly responsible for maintaining the company's internal control structure and for the accuracy, documentation, and submission of all financial reports to the SEC.[314] They must personally certify that the financial reports are accurate and complete.[315]

> Internal control is not "one-size-fits-all," and the nature and extent of controls that are necessary depend, to a great extent, on the size and complexity of the company. Large, complex, multi-national companies, for example, are likely to need extensive and sophisticated internal control systems.[316]

The company's financial reports cannot contain any misrepresentations and the information in the report must be "fairly present[ed]."[317] The CEO and CFO must report any significant deficiencies in the company's internal accounting controls,[318] or any fraud involving the management of the audit committee, and must indicate any material changes in internal accounting controls.[319]

B. Section 404

Section 404 of the Act requires that the management of public companies assess the effectiveness of the company's internal controls over financial reporting and certify in the annual report that those

---

313. Eric Bellman, *Tracking the Numbers / Outside Audit: One More Cost of Sarbanes-Oxley: Outsourcing to India*, WALL ST. J., July 14, 2005, at C1; *see also* Alix Nyberg Stuart, *Sticker Shock*, CFO MAG., Sept. 1, 2003, *available at* http://www.cfo.com/printable/article.cfm/3010299?f=options (indicating that 48% of 200 public companies surveyed will spend at least $500,000 on Sarbanes-Oxley compliance).

314. 15 U.S.C. § 7241(a).

315. *Id.*

316. PCAOB Release No. 2004-001, *supra* note 309, at 9.

317. 15 U.S.C. § 7241(a)(3).

318. *Id.* § 7241(a)(5)(A). Unfortunately, Section 302 does not identify which internal controls must be assessed, leaving it to business executives to decide. However, PCAOB, Release No. 2004-001 states that "[d]etermining which controls should be tested, including controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include: . . . information technology general controls, on which other controls are dependent." PCAOB Release No. 2004-001, *supra* note 309, at A-21.

319. 15 U.S.C. § 7241(a)(5)(B)(6).

controls operate effectively and comply with the requirements of the Act and its related rules and regulations.[320] The assessment also must be reviewed and approved by an outside auditing firm.[321] Some lawyers summarize these sections as requiring management to "look closely and regularly at all the steps taken to ensure the integrity and reliability of the company's financial accounts and tell the public if there is any 'material weakness' in the design or operation of these steps—thereby hopefully avoiding another Enron-like surprise."[322] One securities commentator notes that Section 404 is the one that "seems to have caused the biggest headaches."[323]

The Act requires the SEC to issue rules requiring publicly held companies to include in their annual reports an internal control report containing:

> 1. a statement of management's responsibility for "establishing and maintaining an adequate internal control structure and procedures for financial reporting;"[324] and
>
> 2. an assessment by management at the end of the company's most recent fiscal year "of the effectiveness of the company's internal control structure and procedures . . . for financial reporting."[325]

The SEC has issued rules to implement Section 404.[326] These rules provide that the internal controls[327] subject to assessment by management include but are not limited to:

> controls over initiating, recording, processing, and reconciling account balances, classes of transactions and disclosure and related assertions included in the financial statements; controls related to the initiation and processing of non-routine and non-systematic transactions; controls related to the

320. *Id.* § 7262(a).

321. *Id.* § 7262(b).

322. Michael S. Mensik & Robert Gareis, The Sarbanes-Oxley/Outsourcing Intersection: An Introduction 1 (Sept. 2004), http://www.bakernet.com/NR/rdonlyres/A3C635C0-050C-432F-A30F-3EF65E5D83D1/0/Final_Intersection_SOX.pdf.

323. Saita, *supra* note 297.

324. 15 U.S.C. § 7262(a).

325. *Id.*

326. *See* Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. 36,636 (Securities and Exchange Commission June 18, 2003) (final rule) (codified at 17 C.F.R. pts. 210, 228, 229, 240, 249, 270, and 274) [hereinafter Management's Report].

327. The rules define internal controls to include "policies and procedures that: . . . [p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements." *Id.* at 36,640.

> selection and application of appropriate accounting policies; and controls related to the prevention, identification, and detection of fraud.[328]

Section 404 also requires that every registered public accounting firm that prepares or issues an audit report on a company's annual financial statement attests to, and reports on, the assessment made by management.[329] The Act requires independent auditors to attest to the integrity of a public company's financial controls.[330]

Virtually all financial controls in use today are computer-based and software-controlled. These controls include internal control systems, such as transaction handling and accounting ledgers, and systems linked to third parties such as banks, trading exchanges, and clearinghouses. Any software security breach constitutes a risk to the company's internal financial systems, which could prevent compliance with the requirements of Section 404. Even if the security breach does not directly involve the financial systems, any compromise to the company's IT system could allow an outsider to access the financial system.[331] As such, Section 404 requires the company to sufficiently secure its IT on an enterprise-wide basis so that the independent auditors and corporate executives are willing to attest to the security of the financial systems.

Control Objectives for Information and related Technology (COBIT) was developed by the Information Systems Audit Control Association (ISACA) to provide more specific guidance to companies in developing and assessing IT controls.[332] COBIT addresses internal controls for thirty-four separate IT processes.[333]

In March 2004, the PCAOB published its *Auditing Standards No. 2*, which specifies the "Internal Control—Integrated Framework (1992)," a document prepared by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), as the control frame-

---

328. *Id.* at 36,643.

329. 15 U.S.C. § 7262(b).

330. *Id.*

331. *See* PCAOB Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, ¶ 75 (Mar. 9, 2004), *available at* http://www.pcaobus.org/rules/Release-20040308-1.pdf [hereinafter Auditing Standard No. 2] ("The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting.").

332. For further information on COBIT, see ISACA, http://www.isaca.org/cobit (last visited Feb. 20, 2008).

333. COBIT 4.1 Brochure, *available at* http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf.

work for financial reporting.[334] Although not required by SOX, COSO has quickly become the international standard for managing compliance with the Act.[335]

Auditing Standard No. 2 instructs auditors to focus on two interrelated questions:

1. Was management's assessment of the internal controls "fairly stated, in all material respects"?[336]

2. Did the company, in fact, "maintain[ ], in all material respects, effective internal control over financial reporting"?[337]

C. The CEO's Dilemma

What is a CEO to do? SOX requires that he sign filings with the SEC that certify that the company's computer systems are secure and that the company maintains, in all material respects, effective internal controls over its financial reporting. If he's wrong, he faces potential prosecution for violations of SOX, with personal fines up to one to five million dollars and/or imprisonment for up to ten to twenty years.[338]

Yet, if the company asks its software vendors, whose products the company relies upon to provide that security and effective control, to certify that their systems meet the SOX's requirements, the vendors politely decline, mumbling something about how all software has bugs and the company is not willing to assume the risk that the customer's system may be compromised by hackers, cyberterrorists, or perhaps just a disgruntled ex-employee.

The CEO finds himself between the proverbial rock and a hard place. Thus far the SEC has not taken action against any corporate executives who have signed such an undertaking that later turned out to be untrue. Nor have publicly traded companies raised up with a single voice and demanded better accountability from their vendors. But we have not yet had a major accounting scandal arising from software vulnerabilities.

---

334. Auditing Standard No. 2, *supra* note 331, ¶ 14.

335. *See* Institute of Internal Auditors, *Putting COSO's Theory Into Practice*, TONE AT THE TOP, Nov. 2005, *available at* http://www.theiia.org/download.cfm?file=42122 (calling COSO the industry standard for managing SOX compliance).

336. Auditing Standard No. 2, *supra* note 331, ¶ 167(l).

337. *Id.* ¶ 167(m); *see also* PCAOB Release No. 2004-001, *supra* note 309, at 7 (noting that an attestation of management's evaluation of internal controls "requires the same level of work as an audit of internal control over financial reporting . . . . The auditor, however, also needs to test the effectiveness of internal control to be satisfied that management's conclusion is correct, and therefore, fairly stated.").

338. 18 U.S.C. § 1350(c) (Supp. IV 2006).

VI. SOME ALTERNATIVE AVENUES

The above review of recent developments in tort law indicates that tort law appears to be moving toward a point where at least some types of security-related software vulnerabilities will give rise to tort claims. However, for the most common forms of injury caused by defective security software—loss of sensitive corporate and third party data—the economic loss rule will continue to bar most claims.[339] And, because most security breaches arise from criminal activities, the rules relating to superseding causes may prevent many meritorious tort claims against vendors.[340]

Because of the urgency of the issue, society cannot wait for the courts or legislature to change existing law. As a result, various government agencies and private organizations are looking for alternative avenues to compel software vendors to increase the security of their products.

First, the federal government is a key buyer of security software, acquiring around forty-two percent of all software and computing services.[341] It has the negotiating clout to force software vendors to offer specific warranties that their software is secure, with significant monetary penalties if it is not.[342] While these warranties would appear on their face only to benefit the government, forcing vendors to develop secure software will actually benefit all users, because vendors have strong business reasons to minimize the number of different versions of their software being used. The cost of supporting multiple versions of a single software package is extremely high. As a result, if vendors

339. *See supra* Parts II.F.2, III.D.1.

340. *See supra* Part II.F.1.

341. Of the total IT security software market of $10 billion in 2004, "Federal agencies spent $4.2 billion securing the government's total information technology investment of approximately $59 billion . . . ." OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 2004 REPORT TO CONGRESS, at i (2005).

342. *See, e.g.*, Saita, *supra* note 24 (discussing the influence of the Federal Government in creating a new "model contract" under which vendors must deliver software that meets specific safety requirements); *see also* Federal Information Systems Management Act (FISMA) of 2002, 44 U.S.C. §§ 3541–3549 (Supp. IV 2004) (requiring all federal agencies to follow various security procedures and processes to improve their IT security). In the private sector, large corporations are also using their leverage to negotiate meaningful security-related warranties. *See, e.g.*, *Put It in Writing*, CSO MAG., Oct. 2002, *available at* http://www.csoonline.com/read/100702/writing_528.html (presenting a contract in which GE used its leverage to include language holding its software vendor accountable for the quality of the product); Dennis Fisher, *Contracts Getting Tough on Security*, EWEEK, Apr. 15, 2002, http://www.eweek.com/print_article2/0,1217,a=25494,00.asp (discussing how large companies are using new language in contracts to hold software companies liable for any failures of their product).

are forced to provide more secure versions of their software to the government, it is likely that those versions will be made available to all licensees.[343]

Second, the National Academy of Science and others have proposed that Congress enact legislation that "would increase the exposure of software and system vendors and system operators to liability for system breaches and mandate[ ] reporting of security breaches that could threaten critical societal functions."[344] While no such legislation has yet been considered, a major corporate failure due to defective security software might be the impetus needed for such legislation.

Third, and finally, perhaps one of the most potentially important developments to date is the approach being taken by the Federal Trade Commission (FTC) to address the dangers of computer and network security failures.

Under Section 5(a) of the FTC Act, the agency has a limited mandate to take action against "unfair [or deceptive] acts or practices."[345] The FTC has begun taking action against software users whose systems were breached by hackers and third party confidential information was disclosed. The first case involved a retailer, BJ's Wholesale Club, Inc., whose failure to properly configure its computer system allegedly allowed thousands of customer records to be accessed by cybercriminals who made millions of dollars in fraudulent purchases.[346] The FTC accused the retailer of unfair acts or practices due to its allegedly negligent conduct.[347]

BJ's entered into a consent decree under which it agreed to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the

---

343. Statement of Bruce Schneier, Founder and Chief Technical Officer, Counterpane Internet Security, Inc., Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk: Hearing Before the Subcomm. on Cybersecurity, Science, and Research and Development Comm. of the H. Comm. on Homeland Security 8 (2003), *available at* http://www.ranum.com/security/computer_security/editorials/lawyers/Testimony_Schneier0603.pdf. ("There's a 'rising tide' effect that will happen; once companies deliver products to the increasingly demanding specifications of the government, the same products will be made available to private organizations as well.").

344. *See* NAT'L ACADEMY OF SCIS., CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 14 (2002).

345. 15 U.S.C. § 45(a)(2) (2000).

346. Complaint ¶¶ 7–9, *In re* BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

347. *See id.* ¶ 9 ("Respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers . . . .").

security, confidentiality, and integrity of personal information collected from or about consumers."[348] The FTC has taken action against several other companies for breaches of their systems as well.[349] So far, the jurisdiction of the agency to bring such actions has not been challenged.

If users of insecure software are engaged in deceptive trade practices, and, therefore, subject to FTC enforcement activities, it would not be difficult for the FTC to argue that a vendor who distributes insecure software is similarly engaged in "unfair acts or practices" under the FTC Act. In 2002, the FTC threatened Microsoft that if it did not improve the security of its Passport information service, it could face fines of up to $11,000 per violation, possibly totaling $2.2 trillion.[350] Microsoft took the threat seriously enough to invest a reported $100 million[351] in a security initiative named "Trustworthy Computing," which was claimed to lead to changes in the software development and testing procedures throughout the company.[352] The FTC could begin taking action against vendors of insecure software under Section 5 of the FTC Act. The threat of massive fines

---

348. Decision & Order, *In re* BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

349. *See, e.g.*, *In re* DSW, Inc., No. C-4157 (F.T.C. March 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf (requiring DSW to implement and maintain an information security protocol that is reasonably designed to protect the security, confidentiality, and integrity of personal information regarding DSW's customers).

350. *See* Ashlee Vance, *$2 Trillion Fine for Microsoft Security Snafu?*, THE REGISTER, May 8, 2003, *available at* http://www.theregister.co.uk/2003/05/08/2_trillion_fine_for_microsoft/. The FTC did not accuse Microsoft directly of providing insecure software or services, but instead claimed that Microsoft's stated privacy policies were not accurate regarding security of consumer information. Complaint, *In re* Microsoft Corp., No. 012 3240 (F.T.C. Aug. 8, 2002), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf. The FTC and Microsoft settled the matter with a consent decree under which Microsoft agreed to implement certain security measures and agreed to allow the FTC to monitor its compliance for twenty years. Agreement Containing Consent Order, *In re* Microsoft Corp., No. 012-3240 (F.T.C. Aug. 8, 2002), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftagree.pdf.

351. John Lettice, *Bill Gates Spams the World on Trustworthy Computing*, THE REGISTER, July 19, 2002, *available at* http://www.theregister.co.uk/2002/07/19/bill_gates_spams_the_world/.

352. *See* Robert Lemos, *One Year On, Is Microsoft "Trustworthy"?*, CNETNEWS.COM, Jan. 23, 2003, http://www.news.com/2102-1001_3-981015.html?tag=st.util.print (discussing Microsoft's implementation of the Trustworthy Computing initiative); *see also* Statement of Scott Charney, Chief Trustworthy Computing Strategist for Microsoft, Cybersecurity and Consumer Data: What's at Risk for the Consumer?: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 108th Cong. 30–37 (2003) (discussing issues of cybersecurity and Microsoft's trustworthy computing initiative).

might provide the incentive needed to force vendors to invest the necessary money to make their software secure.

VII. CONCLUSION

Whatever steps are taken by the courts, the legislatures, or government agencies, it is clear that the software security issue is getting progressively worse.[353] It is also clear that most vendors will not take the initiative in this area unless forced to do so by an external force—such as a threat of FTC fines or the specter of large damage awards.[354] "There is no market incentive to produce secure software because software manufacturers risk nothing when their products are insecure."[355] That needs to change.

353. *See, e.g.*, Jaikumar Vijayan & Todd R. Weiss, *List of Data Breaches Grows*, COMPUTERWORLD, June 26, 2006, http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=112230 (discussing a number of recent data compromises and security breaches at large companies).

354. *See* Shawna McAlearney, *Suing for Security*, INFORMATION SECURITY, Nov. 2003, at 16. (quoting attorney Stewart Baker, who has said that "[i]f security problems get worse and worse, juries and judges will be less willing to listen to arguments from software companies and more and more inclined to make them pay for the problems everyone is encountering [based on] the standing of the company in the public eye.").

355. Schneier, *Foreword*, *supra* note 3.