NOTES

TORTS V. CONTRACTS: CAN MICROSOFT BE HELD LIABLE TO HOME CONSUMERS FOR ITS SECURITY FLAWS?

EMILY KUWAHARA*

I. INTRODUCTION

In January 2003, the Slammer worm hit the Internet.[1] Five of the Internet's thirteen root-name servers[2] shut down.[3] Three hundred thousand cable modems in Portugal went offline, all of South Korea's cell phone and Internet services went down, and Continental Airlines cancelled flights from its Newark hub due to its inability to process tickets.[4] It took only six months after the disclosure of a security flaw for a virus writer to write the 376 byte virus.[5] When unleashed, it took ten minutes to infect ninety

* Class of 2007, University of Southern California Gould School of Law; B.S. Interaction Design Engineering 2002, Stanford University; M.A. Telecommunications 2004, Michigan State University. I would like to thank Professor Gregory Keating for his invaluable guidance and fountain of knowledge and the editors of the Southern California Law Review for their hard work and dedication.

1. *E.g.*, Paul Boutin, *Slammed!*, WIRED, July 2003, at 146–47.

2. Root name servers store the internet addresses of all authoritative DNS servers. All computers on the Internet have a numerical address that corresponds to their domain names. The root name server is the server of last resort that a user's computer asks for help in finding the numerical address for a URL such as http://www.usc.edu. The root name server would know what other servers have ".edu" addresses, allowing the URL to be found. For a basic explanation of the Domain Name System (DNS) and the use of root name servers, see generally Daniel Karrenberg, Internet Soc., The Internet Domain Name System Explained for Non-Experts (Feb. 2004), *at* http://www.isoc.org/briefings/016/index.shtml.

3. Boutin, *supra* note 1, at 147.

4. *Id.*

5. *Id.* at 148; *Fighting the Worms of Mass Destruction*, ECONOMIST, Nov. 29, 2003, at 66;

percent of vulnerable systems.[6]

The flaw was a buffer overflow in the Microsoft SQL Server 2000 software.[7] Because the code is embedded in other Microsoft products, not all users were even aware that their systems were running a version of SQL Server.[8] Unfortunately, this was a well-known, preventable security flaw.[9] Moreover, Microsoft had released a patch for the flaw exploited by Slammer six months before the attack.[10] Despite the widespread effects, no flood of lawsuits ensued.[11]

In September 2003, Mary Hamilton filed a class action lawsuit blaming Microsoft for an intrusion by a hacker who stole and used her social security number and financial statements.[12] The case settled under confidential terms.[13]

For either scenario, the case law suggests that the law would not have allowed recovery from Microsoft, despite calls for over twenty years to apply malpractice law, negligence law, and products liability law to

CERT, CERT ADVISORY CA-2003-04 MS-SQL SERVER WORM (Jan. 25, 2003), *at* http://www.cert.org/advisories/CA-2003-04.html. The CERT Coordination Center was established by the Defense Advanced Research Projects Agency at Carnegie Mellon University's Software Engineering Institute, and "identify[ies] and publish[es] preventative security practices, conduct[s] research and provide[s] training to system administrators, managers, and incident response teams." *Information Technology—Essential But Vulnerable: Internet Security Trends: Hearing Before the Subcomm. on Gov't Efficiency, Fin. Mgmt. & Intergovernmental Relations of the H. Comm. on Gov't Reform*, 107th Cong. (2002) [hereinafter *Hearing*] (testimony of Richard D. Pethia, Director, CERT Coordination Center), *available at* http://www.cert.org/congressional_testimony/pethia-11-02/Pethia_testimony_11-19-02.html.

6. *Fighting the Worms of Mass Destruction*, *supra* note 5, at 66.

7. Boutin, *supra* note 1, at 148. A buffer overflow occurs when a program requires a string of characters as input and only allocates a specific amount of memory for it, but fails to check the length of the string that the user actually inputs. *Id.* As a result, when the input is longer than the program's allocated memory for the string, the input literally overflows and writes over the program's own code. This allows the intruder to insert malicious code into the program. *Id.*

8. *Id.* at 147.

9. Paul Festa, *Study says "buffer overflow" is most common security bug*, NEWS.COM, Jan 2, 2002, *at* http://news.com/Study+says+buffer+overflow+is+most+common+security+bug/2100-1001_3-233483.html; Stewart A. Baker & Maury D. Shenk, *A Patch in Time Saves Nine: Liability Risks for Unpatched Software*, BRIEFLY . . . PERSP. ON LEGIS., REG. & LITIG., Nov. 2003, at 1, 3.

10. *See* Baker & Shenk, *supra* note 9, at 1.

11. *See* Mark Rasch, Opinion, *Suing Over Slammer*, SECURITYFOCUS.COM, Feb. 10, 2003, *at* http://www.securityfocus.com/columnists/141.

12. Complaint at 1, 9–10, Hamilton v. Microsoft Corp., No. BC303321 (Cal. Super. Ct. Sept. 30, 2003).

13. Telephone Interview with Dana B. Taschner, Attorney, Law Office of Dana B. Taschner, in L.A., Cal. (Feb. 7, 2006).

software vendors.[14] Amazingly, the substantial arguments that advocate imposing liability have not changed; yet the legal scholarship has not adequately addressed the economic problem of vast liability that concerns the courts. As the world's monopoly power in operating systems,[15] surely Microsoft is the leading candidate for the imposition of products liability, but to date, nothing has happened. Some salient questions arise in the modern era of networked computing. What policy reasons justify suing Microsoft, the world's de facto operating systems provider, when a hacker, a third party, is responsible for creating cyber-chaos? Is products liability an appropriate theory of liability when dealing with bytes? Under any theory of liability, what theories or mechanisms should limit liability, especially when damage can be worldwide?

The problem of cybersecurity is by no means limited to Microsoft; in fact, it may be the most secure system currently available and may never be subject to liability.[16] By using Microsoft, this Note seeks to focus the issue on one type of software in common use. Part II provides background information on cybersecurity, Microsoft's place in the market, and the rise of cyberinsurance. Part III lays out the policy rationales for imposing liability. Part IV describes the current trajectory of the law to the extent that it has addressed this issue and analyzes why it is so problematic. Finally, Part V suggests a mandatory warranty for damages resulting from a security breach where maximum damages are capped.

14. *See* Michael C. Gemignani, *Product Liability and Software*, 8 RUTGERS COMPUTER & TECH. L. J. 173, 187–99 (1982) (exploring the use of negligence and strict liability to hold software vendors liable when software was entered into a computer with punch cards); David A. Hall, Note, *Strict Products Liability and Computer Software: Caveat Vendor*, 4 COMPUTER/L.J. 373, 399–400 (1983) (suggesting the use of strict liability in cases resulting in physical injury when the software that caused the injury is mass-marketed); Michael R. Maule, Comment, *Applying Strict Products Liability to Computer Software*, 27 TULSA L.J. 735, 752 (1992) (advocating for the use of strict liability for software and differentiating between mass-produced software and customized software); Jim Prince, Note, *Negligence: Liability for Defective Software*, 33 OKLA. L. REV. 848, 852–55 (1980) (advocating for the use of strict liability for software because software was distributed in the same manner as other products and was affected by the same policy rationales that underlay products liability). The economic loss doctrine is explicitly excluded from the discussion. *Id.* at 849.

15. Microsoft's share of the market is estimated to be about ninety-four percent. OneStat.com reported it to be ninety-seven percent in 2002. DAN GEER ET AL., COMPUTER AND COMMC'NS INDUS. ASSOC., CYBER INSECURITY: THE COST OF MONOPOLY 12 (2003), *at* http://www.ccianet.org/docs/filings/cybersecurity/cyberinsecurity.pdf.

16. *See* Ira Winkler, Opinion, *Vendor Liability: A Pointless Argument?*, SEARCHSECURITY.COM, Feb. 2, 2005, *at* http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1050897,00.html (arguing that the debate about whether software vendors should be held liable for their security flaws comes a decade too late, given the increased security that is already being implemented in Windows software and the fact that security compromises come from poorly maintained or configured software).

II. BACKGROUND: PERSPECTIVE(S) ON CYBERSECURITY

A. CYBERSECURITY

1. Effects of Cyber Attacks

The prevalence of viruses and worms on the Internet is astounding. An unprotected computer connected to the Internet with no patches, virus scan, or firewall has an estimated forty percent chance of being infected by a "malicious worm" in the first ten minutes, a figure which increases to a ninety-four percent chance in the first hour.[17]

Cybersecurity attacks take various forms: intruders may compromise a computer system by gaining unauthorized access, hackers may install a Trojan horse/malicious code onto a computer using social engineering techniques, automated sniffers may monitor data that travels on a network, automated scanners may scan computers on a network for a known vulnerability, and a distributed denial of service attack may harness the power of millions of unsecured computers to bombard a site with enough data to overload the network.[18] Such attacks may result in a denial of service, unauthorized access to a computer, loss or misappropriation of valuable data, monetary loss, and disruptions to critical health and safety services.[19] Generally, there is also a loss of confidence in computer systems and in the businesses that have been compromised. [20] Most attacks are the result of improperly configured computers or disgruntled employees who gain access to computer resources through inside information, and are not a direct result of programming errors.[21] Yet, as demonstrated by Slammer, when the cause is a programming error, a distributed attack can affect millions of people running the same operating system or software.

17. Tom Zeller, Jr., *Protecting Yourself from Keylogging Thieves*, N.Y. TIMES.COM, Feb. 27, 2006, *at* http://www.nytimes.com/2006/02/27/technology/27hackside.html (citing an estimate of the frequency of cybersecurity breaches by security firm Sophos).

18. *Viruses and Worms: What Can We Do About Them: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations & the Census of the H. Comm. on Gov't Reform*, 108th Cong. (2003) [hereinafter *Viruses Hearing*] (testimony of Richard D. Pethia, Director, CERT Coordination Center), *available at* http://www.cert.org/congressional_testimony/Pethia_testimony_9-10-2003/; CERT, OVERVIEW OF ATTACK TRENDS 1, 3–4 (2002), *at* http://www.cert.org/archive/pdf/attack_trends.pdf.

19. *Hearing*, *supra* note 5; OVERVIEW OF ATTACK TRENDS, *supra* note 18, at 5; *Viruses Hearing*, *supra* note 18.

20. *Viruses Hearing*, *supra* note 18.

21. *See* Jay P. Kesan, Ruperto P. Majuca & William P. Yurcik, *The Evolution of Cyberinsurance*, ACM COMPUTING RESEARCH REPOSITORY cs.CR/0601020 (Jan. 2006); Winkler, *supra* note 16.

2. Criminalization of Hacking

Federal criminal legislation punishes the immediate culprits, hackers.[22] Specifically, it criminalizes knowingly transmitting code that "intentionally causes damages without authorization" and intentionally accessing a computer without authorization and causing damage.[23] The statute further defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[24] Victims also have a civil cause of action against the cyber intruder to "obtain compensatory damages and injunctive relief or other equitable relief."[25]

Congress apparently recognized the tremendous value of our information assets when drafting the definition of "damage" for this statute. They declined, however, to extend liability beyond the criminal hacker by adding, "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."[26]

3. Industry and Scholarly Debate on Liability and Solutions

Though everyone agrees that hacking should result in criminal and civil liability for hackers, the debate about who, if anyone, should bear liability for the underlying security flaw remains contentious. Because this area of law is evolving, the voices of the industry and legal community are particularly salient.

On one end of the spectrum are people like Howard Schmidt, former White House cybersecurity advisor,[27] who opposes liability for software companies because it will raise costs and prices, stifle innovation, and lead

22. 18 U.S.C. § 1030 (Supp. 2002).

23. *Id.* § 1030(a)(5) makes it a crime if one:

> (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage . . . .

24. *Id.* § 1030(e)(8).

25. *Id.* § 1030(g).

26. *Id.*

27. Tom Espiner, *Developers 'Should Be Accountable' for Security Holes*, ZDNET.CO.UK, Oct. 12, 2005, *at* http://news.zdnet.co.uk/software/developer/0,39020387,39228663,00.htm (arguing that software developers should be held personally accountable for the quality of their software, but not legally liable).

to job cuts.[28] He prefers that software vendors use employee incentives and training to encourage the creation of secure code.[29] He characterizes the problem as a quality problem, not one of risk-allocation.

Similarly, while acknowledging that reducing software vulnerabilities is critical to cybersecurity,[30] the Department of Homeland Security rejected governmental regulation in setting security standards for companies, preferring the private sector to self-regulate.[31] Presumably, this includes setting security standards for writing code as well as maintaining a secure corporate environment and networks. This tactic depends on private industry to cooperate in a highly competitive field.

On the other end of the spectrum is Bruce Schneier, a security expert who strongly believes that the cost of insecure software is an externality that should not be borne by users, but by software companies.[32] Market forces have failed because software companies have not made security a priority, leaving users faced with limited purchasing choices.[33] Choices are constrained by software monopolies and the inability to switch from software that uses incompatible proprietary file formats or that requires certain computer system configurations.[34] Perhaps, most importantly, the average consumer is unable to distinguish between a product that truly has superior security and one that claims to have it.[35] In other words, all security defects are latent.

In between are those who advocate for a professional standard for software engineers, who can then be liable for malpractice like doctors, accountants, and lawyers.[36] This idea has little traction.[37] It would require

28. *See* Howard Schmidt, *Give Developers Secure Coding-Ammo*, NEWS.COM, Nov. 3, 2005, *at* http://news.com.com/Give+developers+secure-coding+ammo/2010-1002_3-5929364.html.

29. *Id.*

30. *See* DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE xi (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. The report identifies five priorities for securing the nation's cyberspace. *Id.* at x–xii. The priorities address the issue from multiple angles including reducing existing vulnerabilities in computers, creating a response system, educating and training users about computer security, funding cybersecurity research, and working with other countries to identify hackers and threats. *Id.*

31. *See id.* at ix.

32. Bruce Schneier, Commentary, *Sue Companies, Not Coders*, WIRED.COM, Oct. 20, 2005, *at* http://www.wired.com/news/privacy/0,1848,69247,00.html.

33. *Id.*

34. *Id.*

35. *Id.*

36. Susan Nycum, *Liability for Malfunction of a Computer Program*, 7 RUTGERS COMPUTER & TECH. L.J. 1, 9 (1979).

37. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of*

the professionalization of computer engineering and extensive documentation about the coding and testing process that would bog down production costs and be practically impossible.

Professors Rustad and Koenig suggest the creation of a new tort for software vendors, the negligent enablement of cybercrime.[38] By using a negligence standard, both the software vendor and consumer share the responsibility for maintaining cybersecurity.[39] The software vendor will be liable for "excessive preventable security flaws" and users will be "accountable if they fail to protect passwords or take reasonable steps to implement vendors' security updates."[40]

The professors reject the extension of products liability doctrine to software vendors, primarily because the courts have not been receptive to its application.[41] Specifically, they note the retreat from a strict liability standard to a negligence standard in the *Restatement (Third) of Torts: Products Liability* and believe that a return to products liability is unlikely.[42] Furthermore, the economic loss doctrine precludes recovery for the financial damage resulting from a security breach because there is often no physical injury or harm to other property.[43] They conclude that "[c]ourts may be more willing to recognize a negligent enablement theory of product liability where prior similar computer intrusions signal a software manufacturer's ill-considered design decisions."[44] Why courts may favor this negligence theory over strict products liability theory for the same purely economic damage remains unclear.[45] Given the widespread effects of a distributed attack, courts may be reluctant to extend liability to cover all victims of an attack for fear of unlimited liability. One of the chief

Cybercrime, 20 BERKELEY TECH. L.J. 1553, 1590–91 (2005) (stating that courts do not recognize a professional standard of care for software engineers). This idea has also been suggested for over twenty years and no professionalization of computer engineers has truly occurred in that time. *See, e.g.*, Gemignani, *supra* note 14, at 190.

38. Rustad & Koenig, *supra* note 37, at 1557.

39. *Id.* at 1561.

40. *Id.* at 1576–80.

41. *Id.* The authors note that strict liability has been extended to products that incorporate software but not to stand-alone software. *Id.* at 1579.

42. *Id.* at 1577.

43. *Id.* at 1580.

44. *Id.*

45. In *Hou-Tex, Inc. v. Landmark Graphics*, a defective software case, the court found that "the fact of most import" was that Hou-Tex suffered only economic loss and thus could not recover under a claim of negligence. Hou-Tex, Inc. v. Landmark Graphics, 26 S.W.3d 103, 107 (Tex. App. 2000). The court reasoned that permitting recovery for economic loss would "disrupt the risk allocations" provided for in the license agreement. *Id.*

concerns about excessive products liability is the ability of companies to assess their risk of liability and function efficiently.[46] The concern is equally applicable here.

Rustad and Koenig speculate that courts may require a showing of foreseeability or notice to the software vendor that a cybercrime may occur to establish a breach of duty, as a way to limit litigation and liability.[47] This requirement, however, only makes it more difficult for plaintiffs who are not security experts to bring suit, while doing nothing to limit damages for a widespread Slammer-like attack.

In essence, the tort of negligent enablement diverges from a products liability analysis in its use of a duty of care. Though imposing a negligence standard may spur the creation of a standard level of care for programmers, creating a standard of care too early in the evolution of software may prompt companies to hew closely to the standard to minimize liability risks instead of pursuing novel solutions that actually improve security.[48] If the evolution of the standard level of care for secure programming parallels the development of the level of care required for financial institutions for safeguarding data, the standard will require due care in creating and following security procedures, not in utilizing specific types of security products.[49] Due care will be defined as showing consideration for security in the design phase, documentation of coding, and rigorous testing. If so, security flaws will continue to exist regardless of the exercise of due care.[50] A bug does not imply that procedure was not followed but merely that the bug was not caught.

Strict liability has been suggested since the inception of the computer revolution though the arguments have failed to address the economic loss

46. Alan Schwartz, *The Case Against Strict Liability*, *in* A PRODUCTS LIABILITY ANTHOLOGY, 207, 211 (Anita Bernstein ed., 1995).

47. Rustad & Koenig, *supra* note 37, at 1583–84.

48. *See* NAT'L ACAD. OF ENG'G, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 52 (2003), *at* http://www.nap/edu/catalog/10685.html. Though Judge Learned Hand in *T.J. Hooper* dismissed the industry standard as inconclusive of negligence, in a complex industry such as software, it is easy to imagine that judges would prefer to defer to the software industry's judgment. *See* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932).

49. *Information Security Duty of Care Evolving: Encryption Not Common, Standard is Elusive*, 74 U.S.L.W. 2516, 2517 (2006). The Gramm-Leach-Bliley Act imposes a duty on financial institutions to secure their customers' financial data. 15 U.S.C. § 6801(b) (2000).

50. Gemignani, *supra* note 14, at 191 (stating that res ipsa loquitur cannot be applied to a computer malfunction because a bug in a complex program does not necessarily imply lack of due care).

doctrine.[51] The characterization of computer software and the rationales given for and against strict liability have changed little. "If, indeed, a technology is so sophisticated that no one fully understands or is able to control it, but is so necessary that modern society must employ it, then it would seem that the risks inherent in its use ought to be spread evenly among all the users."[52] The same author notes, however, that the utility of software may be so great that the cost of individual harm is preferable to making software prohibitively expensive by imposing liability on vendors.[53]

Professors Lichtman and Posner suggest holding Internet service providers liable for malicious code that they help disseminate.[54] Other commentators propose imposing liability on end-users, namely, consumers and corporations that fail to patch and maintain their computers' security[55] and that inadvertently transmit malicious code.[56] As demonstrated by Slammer, the Internet's security depends on the security of all its components. Holding such parties liable presumes that Microsoft fulfills its obligations by continuously rolling out patches and assumes that any virus was unleashed after the patch. The feasibility of suing all of these defendants and recovering, however, appears minimal, if not impossible.[57]

51. *E.g.*, *id.* at 203.

52. *Id.* at 197.

53. *Id.* at 202.

54. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222 (2006).

55. *See generally* Baker & Shenk, *supra* note 9, at 17–23 (discussing the possible impact of imposing such liability); Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43 (2002); Sarah Faulkner, Comment, *Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1019, 1028 (2000).

56. *See* Meiring de Villiers, *Computer Viruses and Civil Liability: A Conceptual Framework*, 40 TORT TRIAL & INS. PRAC. L.J. 123, 124 (2004).

57. *See* Rasch, *supra* note 11.

B. MICROSOFT'S SPECIAL PLACE[58]

1. Microsoft's Market

Microsoft's market share in operating systems is estimated to exceed ninety percent.[59] In 2005, its revenue was $39.79 billion, a nearly $3 billion increase from the previous year.[60] Approximately $12 billion came from its Client division which encompasses standard versions of the Windows operating system: XP, Professional, Home, Media Center, and Tablet PC.[61] Over eighty percent of this revenue comes from the licensing of pre-installed Windows on new personal computers.[62] The Server and Tools division, which includes Windows Server, Windows Exchange Server, and Windows SQL server accounted for over $9.8 billion in revenue through one-time and multi-year licensing agreements.[63]

2. Microsoft's Security Woes

In January 2002, Microsoft launched the Trust Worthy Computing Initiative in an effort to place a high company-wide priority on the security of its products. [64] Since 2002, Microsoft has implemented the automatic installation of patches,[65] unveiled a service that provided updates, antivirus

58. Microsoft is not the only major private player suffering from security flaws. In mid-2005, a security research analyst revealed that the "infrastructure operating system" (IOS) that controlled Cisco's routers contained a security flaw that, if exploited, could have brought down the nation's information infrastructure. Kim Zetter, *Cisco Security Hole a Whopper*, WIRED.COM, July 27, 2005, *at* http://www.wired.com/news/privacy/0,1848,68328,00.html. Routers direct traffic on the Internet. *Id.* The security analyst decided to present this flaw at a security conference after the source code for the IOS was stolen for the second time. *Id.* Like Microsoft, Cisco commands a majority of the router market and a vulnerability in a Cisco product implies severe ramifications for the Internet's backbone. *Id.* This Note's analysis of Microsoft's position in the market and consequent liability also applies to similarly situated players like Cisco.

59. Microsoft's share of the market is estimated to be about ninety-four percent. OneStat.com reported the market share to be ninety-seven percent in 2002. GEER ET AL., *supra*, note 15, at 12.

60. MICROSOFT CORP., 2005 ANNUAL REPORT 2 (2005), *available at* http://www.microsoft.com/msft/ ar05/downloads/MS_2005_AR.doc.

61. *Id.* at 24.

62. *Id.*

63. *Id.* at 25.

64. MICROSOFT CORP., Q&A: HOW MICROSOFT IS REFOCUSING ON SECURITY, RELIABILITY, PRIVACY, AND MORE, AS PART OF TRUSTWORTHY COMPUTING INITIATIVE (Feb. 20, 2002), *at* http://www.microsoft.com/presspass/features/2002/feb02/02-20mundieqa.mspx.

65. *See* MICROSOFT CORP., THE JOURNEY TO TRUSTWORTHY COMPUTING: MICROSOFT EXECS REPORT FIRST-YEAR PROGRESS (Jan. 15, 2003), *at* http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.mspx.

protection, and data backup support,[66] and trained its developers to write more secure code.[67]

Despite increased efforts, in 2003, the Computer and Communications Industry Association published a report that bluntly put a "special burden . . . upon Microsoft because of [the] ubiquity of its product."[68] The authors of the report blamed Microsoft for the security risk inherent in a Microsoft monopoly world where virtually all computer users are prone to the same attack at the same time.[69] The root of this problem, the report says, is Microsoft's practice of integrating its products to the point of unmanageable complexity, resulting in inevitable security flaws, and also, ironically, user lock-in.[70]

Other experts agree. Because most software designers focus on usability and user needs, security and reliability tend not to get the attention they merit in the design phase.[71] As a result, many computer systems are inherently unstable and unreliable, creating the largest security vulnerability of our current network.[72] Microsoft's early promotions of its products reflected its strong priority on user-friendly design and integration. In its 1996 Annual Report, Microsoft's Chairman Bill Gates lauded the accomplishments of Windows 95 as "ease of use, 32-bit applications, and increased productivity" and boasted that its research and development was "driven by customer feedback."[73]

66. *See* MICROSOFT CORP., MICROSOFT ANNOUNCES PRICING AND LICENSING DETAILS FOR WINDOWS ONECARE LIVE (Feb. 7, 2006), *at* http://www.microsoft.com/presspass/press/2006/feb06/02-07OneCarePricingPR.mspx.

67. MICROSOFT CORP., Q&A: TRUSTWORTHY COMPUTING AT FIVE YEARS (Jan. 16, 2007), *at* http://www.microsoft.com/presspass/features/2007/jan07/01-16twc.mspx.

68. GEER ET AL., *supra* note 15, at 3.

69. *Id.* at 12.

70. *Id.* The Computer Technology Industry Association put out a statement saying that the root cause is not Microsoft's monoculture but human error and suggested increasing security training for IT workers. Joanna Glasner, *Want PC Security? Diversify*, WIRED.COM, Sept. 25, 2003, *at* http://www.wired.com/techbiz/it/news/2005/09/60579.

71. *See* Abraham D. Sofaer & Seymour E. Goodman, *Cyber Crime and Security: The Transnational Dimension*, *in* THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 1, 20 (Abraham D. Sofaer & Seymour E. Goodman eds., 2001).

72. *See id.* at 19–20.

73. MICROSOFT CORP., 1996 MICROSOFT ANNUAL REPORT 3 (1996). In fact, the company's vision for the Internet and its software was "[i]ntegrated software that integrates everything else" so that it would be "nearly impossible for our customers to know exactly where their desktops end and the Internet begins." *Id.* at 9. Windows 98 also touted the same "great software that helps people work, communicate, and learn." MICROSOFT CORP., 1998 MICROSOFT ANNUAL REPORT 3 (1998). Most of Microsoft's research and development remained focused on "making our products easier to use, even as the underlying software grows more complex, so our customers don't have to learn as many utilities and commands." *Id.* at 5. In contrast, in its most recent 2004 and 2005 annual reports, Microsoft's Bill

The year 2003 proved to be a trying one for Microsoft. Slammer hit in January.[74] In August, the SoBig and Blaster worms attacked Windows computers, reportedly costing an estimated $35 billion in damage.[75] If this is an accurate estimate, it exceeded Microsoft's 2003 revenue.[76] Finally, in September 2003, Mary Hamilton filed a class action suit under California Unfair Business Practice Laws.[77]

The Hamilton complaint alleged that Microsoft's inadequate security and ineffective notice of security risks facilitated unauthorized access to her Windows-operated computer.[78] Hamilton suffered from identify theft after a hacker gained access to her computer and maliciously used her personal financial information and her social security number.[79] The complaint posited that Microsoft's "eclipsing dominance in desktop software has created a global security risk"[80] by creating "excessive complexity and, consequently, vulnerability" with its product integration.[81] It also characterized the security alerts put out by Microsoft as too complex for a member of the general public to understand.[82]

After the Hamilton class action was filed, Microsoft suffered a staggering drop in stock prices.[83] As noted by Hamilton's attorney, Dana

Gates included privacy and security as among Microsoft's chief concerns and goals. MICROSOFT CORP., 2005 MICROSOFT ANNUAL REPORT, *supra* note 60, at 3; MICROSOFT CORP., 2004 MICROSOFT ANNUAL REPORT 2 (2004). Microsoft's change in focus has been noticed. At a trade show in November 2003, Microsoft unveiled security-related programs, a stark contrast from the "glitzy" products of earlier years. *Fighting the Worms of Mass Destruction*, *supra* note 6, at 65.

74. Boutin, *supra* note 1, at 146.

75. *Fighting the Worms of Mass Destruction*, *supra* note 6, at 65. The SoBig worm propagated through email attachments that recipients or email programs inadvertently opened. CERT, CERT INCIDENT NOTE IN-2003-03 (Aug. 22, 2003), *at* http://www.cert.org/incident_notes/IN-2003-03.html. The Blaster worm exploited a buffer overflow in Microsoft Windows and performed a denial of service attack on www.windowsupdate.com, preventing users from patching the security flaw. CERT, CERT ADVISORY CA-2003-20 W32/BLASTER WORM (Aug. 14, 2003), *at* http://www.cert.org/advisories/CA-2003-20.html.

76. MICROSOFT CORP., 2004 ANNUAL REPORT, *supra* note 73, at 5.

77. Complaint, *supra* note 12, at 14–17. Dana Taschner, attorney for plaintiff, filed suit under California's Unfair Business Practice statute because the law remains unfavorable to products liability. Telephone Interview with Dana B. Taschner, *supra* note 13. He believes "if they put out a product into the stream of commerce without disclosure [Microsoft] should be liable under products liability." *Id.*

78. Complaint, *supra* note 12 at 9–10.

79. *Id.*; Interview by Bill Hemmer with Mary Hamilton and Dana Taschner, Attorney, Law Offices of Dana B. Taschner, on *American Morning* (CNN television broadcast on Nov. 6, 2003), *at* http://transcripts.cnn.com/TRANSCRIPTS/0311/06/ltm.12.html.

80. Complaint, *supra* note 12 at 7.

81. *Id.* at 8.

82. *Id.* at 10.

83. Reed Stevenson, *Microsoft Security Flaws Infecting Its Finances*, FORBES.COM, Oct. 24, 2003, *at* http://www.forbes.com/newswire/2003/10/24/rtr1122772.html. The article reports the

Taschner, the primary risk to Microsoft from a lawsuit alleging insufficient cybersecurity lies not in being exposed to liability per se, but in the consequent drop in stock price if it is ever held liable.[84] Consequently, he predicted that Microsoft will settle any security related case prior to trial because Microsoft's board prefers to avoid the possibility of a precedent-setting adverse final judgment.[85] The Hamilton case was dismissed with prejudice in April of 2004 under confidential settlement terms.[86] The prospects of creating any case law with the software giant are appealing, but chances remain slim.

For the first time in 2005, Microsoft's Annual 10-K report acknowledged the risk of reduced revenues and potential liability due to security flaws, partially blaming its own dominance in the market place: "While this is an industry-wide phenomenon that affects computers across all platforms, it affects our products in particular because hackers tend to focus their efforts on the most popular operating systems and programs and we expect them to continue to do so."[87] Microsoft also stressed its invigorated efforts to boost security with a long string of steps it was taking to address security concerns, before admitting "[n]evertheless, actual or perceived vulnerabilities may lead to claims against us. While our license agreements typically contain provisions that eliminate or limit our exposure to such liability claims, there is no assurance these provisions will be held effective under applicable laws and judicial decisions."[88] Whether liability is ever imposed or not, the specter of liability exists and appears to be motivating Microsoft to improve its security.

In 2007, Microsoft released a new operating system, Microsoft Vista, which promised "significant advances in security, digital media, user interfaces, and other areas that are expected to enhance the user and

"sharpest drop in Microsoft's share price since Sept. 17, 2001, the day the markets reopened after the World Trade Center attacks." *Id.*

84. Telephone Interview with Dana B. Taschner, *supra* note 13. This observation is supported by several studies that suggest that product recalls and litigation negatively affect the stock prices of the manufacturers. The drop in stock price reflects the market's determination of the price of the litigation. MICHAEL J. MOORE & W. KIP VISCUSI, PRODUCT LIABILITY ENTERING THE TWENTY-FIRST CENTURY: THE U.S. PERSPECTIVE 27 (2001).

85. Telephone Interview with Dana B. Taschner, *supra* note 13. Taschner estimates that Microsoft's legal department is approximately 200–300 attorneys, larger than many law firms. Microsoft also brought in outside counsel, Ron Olson of Munger, Tolles, and Olson, to litigate this case. *Id.* The realities of suing a giant such as Microsoft cannot easily be dismissed when debating theories of liability against software manufacturers.

86. Telephone Interview with Dana B. Taschner, *supra* note 13.

87. MICROSOFT CORP., 2005 ANNUAL REPORT (FORM 10-K) 14 (June 30, 2005).

88. *Id.*

developer experience."[89] Vista touts many security enhancements, which if they work, will dramatically decrease the potency and probability of cyber attacks.[90] The operating system, however, is highly complex, containing an estimated fifty million lines of code, and the release of Vista was delayed for security and quality control reasons.[91]

C. THE RISE OF CYBERINSURANCE

The burgeoning cyberinsurance industry signals the increase of risk for companies that rely heavily on computers. The economic loss is high enough that companies seek to redistribute the risk to an insurance company. Until recently, corporations and insurance companies relied on general liability policies to cover computer compromises.[92] Starting in the late 1990s, however, insurance companies created stand-alone policies for hacker and/or cyber insurance.[93]

Revealed in 2000, one of the most comprehensive cyber policies is provided through AIG. The most current policy includes coverage for the loss of information assets and business interruption from a failure of security.[94] Notably, the policy excludes any failure to "take reasonable

89. *Id.*; MICROSOFT CORP., MICROSOFT LAUNCHES WINDOWS VISTA AND MICROSOFT OFFICE 2007 TO CONSUMERS WORLDWIDE (Jan. 29, 2007), *at* http://www.microsoft.com/Presspass/press/2007/jan07/01-29VistaLaunchPR.mspx.

90. TONY NORTHUP, MICROSOFT CORP., WINDOWS VISTA SECURITY AND DATA PROTECTION IMPROVEMENTS (June 1, 2005), *at* http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx.

91. Steve Lohr & Laurie J. Flynn, *Microsoft to Delay Next Version of Windows*, N.Y. TIMES.COM, Mar. 22, 2006, *available at* http://www.nytimes.com/2006/03/22/technology/22soft.html.

92. Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USATODAY.COM, Feb. 9, 2003, *available at* http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm.

93. *See id.*; Majuca, Yurcik & Kesan, *supra* note 21, at 4.

94. AMERICAN INTERNATIONAL SPECIALTY LINES INSURANCE COMPANY, AIG NETADVANTAGE SECURITY INTERNET & NETWORK SECURITY INSURANCE 1–2 (Mar. 2003), *at* http://www.aignationalunion.com/nationalunion/public/natfiledownload/0,2138,2734,00.pdf. A failure of security is defined as:

> (1) the actual failure and inability of the security of your computer system to mitigate loss from or prevent a computer attack;
> (2) with respect to [Security Liability Coverage] only, physical theft of hardware or firmware controlled by you (or components thereof) on which electronic data is stored, by a person other than an insured, from a premises occupied and controlled by you; or
> (3) with respect to dependent business interruption only, the actual failure and inability of the security of your dependent business' computer system to prevent a computer attack.
> Failure(s) of security shall also include such actual failure and inability above, resulting from the theft of a password or access code by non-electronic means in direct violation of your specific written security policies or procedures.
> However, in no event, shall any of the above constitute a failure of security if resulting from operational errors, unintentional programming errors, or any failure in project planning.

Id. at 6. "Unintentional programming errors" is not defined. *Id.*

steps, to use, design, maintain and upgrade your security."[95] Furthermore, cyberinsurance companies generally require an auditing of a company's security procedures at the time of application and the company is further required to follow them in order to recover.[96] This almost eliminates the first-party insurance externality of consumers who fail to take precautions because they are insured[97] and sets standard levels of security that insurers tie to risk and pricing. Because the critical issue in assessing the feasibility of imposing liability on Microsoft is the scope of exposure to liability, cyberinsurance policies are highly informative of ways to address the insurance problems inherent in a heterogeneous pool of consumers.

Cyberinsurance may be the most effective tool for managing the economic risk of a security failure for larger companies or companies that rely heavily on computer networks.[98] Given the utility provided by Microsoft's operating system and the impossibility of Microsoft to insure all of these business users against security threats, cyberinsurance is the most appropriate solution for redistribution of risk for the business user.[99]

Despite its appeal as a solution for business users, cyberinsurance fails to cover the rather large, but unsophisticated consumer base of home users. Unsurprisingly, identity theft insurance is a burgeoning new industry. Identity theft insurance can now be purchased through home owner's insurance, as a stand-alone policy, or from banks and credit card companies.[100] The average policy costs $25–50 and covers $15,000–$25,000 worth of "lost wages, phone calls, notary fees, and sometimes attorney's fees."[101] Critics of identity theft insurance say that the costs outweigh the benefits because the average cost of out-of-pocket expenses

95. *Id.* at 14.

96. *See* Jay P. Kesan, Rupterto P. Majuca & William J. Yurcik, *The Economic Case for Cyberinsurance* 27–28 (Univ. of Ill. Coll. of Law, Working Paper No. 2, 2004), *available at* http://law.bepress.com/uiuclwps/papers/art2/ (detailing the different methods by which insurance companies tied their customers to an appropriate level of risk).

97. *See* Steven P. Croley & Jon D. Hanson, *Rescuing the Revolution: The Revived Case for Enterprise Liability*, 91 MICH. L. REV. 683, 793 (1993) (discussing externalities in insurance).

98. *See* Robert Steinberg, *Advising Clients About Hacker Insurance*, 25-Feb L.A. LAW. 60, 60 (2003).

99. *See* Kesan, Majuca & Yurcik, *supra* note 96, at 19 (discussing the economic arguments for using a market remedy, namely cyberinsurance in lieu of torts and regulation to deal with security issues).

100. *See* Jennifer Lynch, Note, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 283–84 (2005).

101. *Id.*; Sandra Block, *More Uneasy Consumers Purchase Identity Theft Insurance*, USATODAY.COM, MAY 5, 2003, *available at* http://www.usatoday.com/money/perfi/columnist/block/2003-05-05-ym_x.htm.

for victims of identity theft was $1000 in 2003, the average time spent was twenty-two work days, and only sixteen percent of victims faced false criminal histories that required an attorney to clean up.[102] Unlike cyberinsurance policies for businesses, it is not clear whether identity theft insurance redistributes the risk efficiently or whether consumers are overpaying to cover a risk they never should have had to face. Such policies do not cover data loss that may also occur in a cyber attack. Imposing liability on Microsoft may be a way for home users to recoup some of their losses when fault can be assigned to Microsoft.

III. POLICY RATIONALES FOR ALLOCATING RISK TO MICROSOFT

As detailed below, courts are generally reluctant to allow recovery for economic losses and seem to have rejected the few opportunities to expand products liability law to software.[103] Though legitimate concerns about unmanageable litigation and prohibitive liability exist, the policy reasons for allowing recovery from a software monopoly remain compelling. The decision to impose tort liability on software manufacturers will be primarily based on policy considerations.[104]

A. COMPENSATION OF VICTIMS

Barring situations in which cyberinsurance adequately compensates for losses, tort law may be the only source of compensation for ordinary victims of a security breach.[105] A business user is likely to have insurance, but the average unsophisticated user may not. Most malicious programmers may never be caught and even if they are, are likely to be insolvent.[106] If a hacker fortuitously has money, legislation currently allows for recovery from this defendant.[107]

B. DETERRENT EFFECT V. MARKET FORCES

Due to Microsoft's virtual monopoly on the operating systems market, market forces may not provide sufficient incentive to institute higher

102. *See* David Simons, *ID Theft Insurance Isn't Insurance*, FORBES.COM, May 29, 2003, *at* http://www.forbes.com/2003/05/29/cx_ds_0529simons.html.

103. *See infra* text accompanying notes 210–216.

104. *E.g.*, NAT'L ACAD. OF ENG'G, *supra* note 48, at 46.

105. *E.g.*, *id.* at 43–44.

106. *E.g.*, *id.*

107. 18 U.S.C. § 1030(g) (Supp. 2002).

security standards and programming procedures. Starting in 2002, Microsoft recognized the demand for secure products and shifted some of its energy toward securing its products.[108] The newest operating system, Windows Vista, touts improved security and integrated security measures over its predecessors.[109] Skeptics of the tort system would argue that these steps are sufficient and demonstrate that the market works.

Microsoft, however, is a virtual monopoly. If the charges in the report published by Computer and Communications Industry Association are correct, then Microsoft's monopoly power comes from its ability to lock-in products through aggressive integration of its programs and its operating systems.[110] As such, it has little incentive to overhaul its operating system to meet a higher standard of security. Such an overhaul would inevitably be a costly process, which would be strongly resisted by Microsoft, and final costs may indeed fall to the consumer. Microsoft's best business move is to improve the security of its operating systems without losing its ability to integrate products, thereby fending off charges that its system architecture is faulty. Regardless of whether liability is ever imposed, the specter of liability will keep Microsoft racing to improve its security in order to maintain its stronghold on the market.

C. RISK BEARING

Imposition of liability under tort law often reflects the public policy determination that one party is the superior risk bearer.[111] Though Microsoft repeatedly reminds the public that the hacker is the proximate cause,[112] Microsoft possesses exclusive control over the code and the best knowledge of how to design a system to prevent an attack. Between the consumer and itself, Microsoft is the better bearer of risk.

Critics of strict liability charge that when customers do not bear the

108. *See* Todd Bishop, *Should Microsoft Be Liable for Bugs?*, SEATTLE POST-INTELLIGENCER, Sept. 12, 2003, *available at* http://seattlepi.nwsource.com/business/139286_msftliability12.html; MICROSOFT CORP., Q&A: HOW MICROSOFT IS REFOCUSING ON SECURITY, RELIABILITY, PRIVACY, AND MORE, AS PART OF TRUSTWORTHY COMPUTING INITIATIVE, *supra* note 64.

109. MICROSOFT CORP., Q&A: TRUSTWORTHY COMPUTING AT FIVE YEARS, *supra* note 67.

110. GEER ET AL., *supra* note 15, at 13–14.

111. This cost benefit analysis originates from Learned Hand's B<pL analysis in *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947). Liability depended upon whether the burden of adequate precautions exceeded the probability of the risk multiplied by the gravity of the harm. *Id.*

112. MICROSOFT CORP., 2005 ANNUAL REPORT (FORM 10-K), *supra* note 87, at 14; Interview by Bill Hemmer, *supra* note 79.

risk of harm, morale hazard increases.[113] Morale hazard is the increased danger created by consumers who become more reckless in their conduct because they are insured against loss.[114] In this case, however, consumers have no incentive to change their behaviors. Consumers have no information about Microsoft's closed source code that will allow them to assess the risk of using their computer on any given day. In fact, the average consumer is unable to judge ex ante whether a cyber attack's root cause is Microsoft's failure to write secure code, or the user's inadvertent visit to an infected website, or simply the insecurity of millions of other computers. This uncertainty leaves users only the option to do less computing to avoid costly computer infections.

Some questions remain as to whether consumers should have to take such measures to avoid the risk. The three factors often used to determine the superior risk bearer are unknown and vary for each security flaw: the burden of adequate precautions, probability of the risk, and the gravity of the harm.[115]

D. ESTABLISHMENT OF STANDARD OF CARE

If a negligence system imposed liability on Microsoft, then a breach of duty and accompanying standard of care must be established. This may provide a catalyst for the industry to create a self-imposed standard of care because compliance with industry standards is often, though not always, indicative of a lack of breach.[116] Software developers protest liability, justifying their faulty software by stating that software is inherently insecure and claiming that it would be patently unfair to sue them for an impossible dream.[117]

The excuse sounds familiar. The American automobile industry once blamed drivers and roads instead of itself.[118] Though accidents still occur, standards for car safety have undeniably improved from the auto industry's exposure to products liability and regulation.[119] The same holds true for

113. *See, e.g.*, Mehr, Cammack & Rose, *Principles of Insurance*, *in* TORT AND ACCIDENT LAW 724, 727 (Robert E. Keeton, Lewis D. Sargentich & Gregory C. Keating eds., 4th ed. 2004).

114. *See id.*

115. *Carroll Towing*, 159 F.2d at 173.

116. *See The T.J. Hooper*, 60 F.2d 737, 740 (2d Cir. 1932).

117. *See* Bishop, *supra* note 108; Declan McCullagh, *A Legal Fix for Software Flaws?*, CNET NEWS.COM, Aug. 26, 2003, *at* http://news.com.com/A+legal+fix+for+software+flaws/2100-1002_3-5067873.html.

118. Rustad & Koenig, *supra* note 37, at 1608.

119. *Id.*

operating systems.[120]

Liability cannot miraculously force the creation of a perfect operating system. It does, however, shift the risk-benefit analysis to Microsoft and forces it to balance the risk of distributing potentially insecure software and the risk of litigation. Microsoft's rise to dominance in the operating systems marketplace should be lauded. But when one company holds the key to the security of ninety percent of the world's personal computers, regardless of whether the software can ever be perfect, it assumes a responsibility, and the risk-benefit analysis of selling new products should be shifted to it.

E. RELATIONSHIP WITH CONTRACT LAW

A principal concern behind criticisms of products liability is the fear that "contract law would drown in a sea of tort."[121] Admittedly, by allowing recovery for security breaches by hackers, one is reallocating the risk of a cyber breach onto the manufacturer, after the manufacturer carefully contracted it away. This reduces certainty for the manufacturer and undermines the contract.

Contract law presumes bargaining by both parties.[122] When ninety percent of the world's computers run Microsoft Windows, where Windows is pre-installed on the majority of new computers, and where consumers are not expected to understand how to install a different operating system, the contract can be said to be an incredibly one-sided and unconscionable form contract. The present warranty may keep the price of the operating system down, though in a virtual monopoly, the extent to which a warranty affects the price is unknown. Furthermore, consumers are already shouldering the price of faulty security and are paying out-of-pocket costs in the event of data loss, identity theft, and in the form of third party software to prevent such losses.[123]

Microsoft will never opt to provide a warranty to cover any losses and consumers have very little choice but to accept its terms. In this case, products liability theory appropriately reallocates the risk from the consumer to Microsoft.

In the alternative, as discussed below, laws can be created to mandate

120. *See* Schneier, *supra* note 32.
121. E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 866 (1986).
122. W.DAVID SLAWSON, BINDING PROMISES 23 (1996).
123. *See* Schneier, *supra* note 32.

an effective warranty to resolve the issue under contract law.[124]

F. LIABILITY INSURANCE COSTS

One criticism of products liability is that it raises a manufacturer's liability insurance to a prohibitive level, thus unfairly encumbering software companies and driving them out of business. The fear, however, that liability will lead to higher liability insurance premiums for software vendors and to an eradication of small start-ups may not pan out. A smaller company's premium will likely not be as high as Microsoft's because its potential exposure to liability will be lower.[125] Some security experts argue that society has become so dependant upon software that this additional cost of liability insurance is justified in light of the security risks.[126]

G. IMPACT ON INNOVATION

Another frequent argument against imposing liability on Microsoft is that Microsoft may decide to delay or discontinue an innovative development due to security concerns and consequent exposure to liability.[127] In this age of network and computer dependency, erring in favor of securing the world's data may be a necessary result. The Department of Homeland Security (DHS) called cyberspace the "control system of our country" and notes that by 2003, the country was dependent upon information infrastructure.[128]

Since liability for inadequate safety and regulations have been imposed on automobile manufacturers, the number of fatalities from automobile accidents has dramatically decreased.[129] Arguably, automobile safety encourages more drivers to drive cars. Similarly, increased cybersecurity will encourage more online transactions and innovations in cyberspace.[130] Trust is a cornerstone of business and whatever innovations Microsoft must forgo to foster more trust in innovations in cyberspace may

124. *See*, *infra* Part V.

125. *Fighting the Worms of Mass Destruction*, *supra* note 6, at 67.

126. *Id.*

127. *See* Mary Kirwan, Column, *Decrypting the Future of Security*, GLOBEANDMAIL.COM, Mar. 18, 2005, *at* http://www.theglobeandmail.com/servlet/story/RTGAM.20050311.gtkirwanmar11/BNStory/Technology/ (reporting that the Microsoft lawyers at the RSA Security conference vehemently opposed liability because liability would kill innovation).

128. DEP'T OF HOMELAND SEC., *supra* note 30, at 1.

129. CARL T. BOGUS, WHY LAWSUITS ARE GOOD FOR AMERICA 141 (2001).

130. Loss of trust in the online environment troubles the computing industry. *See* Kirwan, *supra* note 127 (reporting industry concerns from the 2005 RSA Security Conference).

be a necessary price to pay.

H. DISCLOSURE OF SECURITY FLAWS IS INSUFFICIENT

Some opponents of liability tout the idea that disclosure of security flaws is sufficient. Richard Clarke, former White House cybersecurity and counterterrorism adviser, suggested holding Microsoft and other software companies publicly accountable by asking them to disclose their quality-assurance practices.[131] He suggests that the industry should then create its own best practices which will be used to measure each company's performance.[132]

This solution depends upon software providers to disclose information that they have no incentive to disclose. Furthermore, Microsoft's disclosure of its security practices does not change the reality that consumers have no actionable options because it is a virtual monopoly.

In sum, persuasive policy arguments exist for imposing liability on Microsoft. Because tort liability is often about balancing various factors to create the proper cocktail of optimal deterrence, increased safety, and victim compensation, the true difficulty lies in ascertaining the probability of an attack, the magnitude of harms, and the progression of technological solutions.[133]

IV. CURRENT (NON)-LIABILITY FOR SOFTWARE DEFECTS

Under current law, suing Microsoft on a products liability theory is virtually impossible.[134] Far from being conclusive evidence that consumers should not be able to sue Microsoft, the inability of the debate to move forward suggests that the current legal framework for analyzing software concerns is inadequate. The developing case law is described below to illustrate the difficulties inherent in the law's current trajectory.

A. IS SOFTWARE A PRODUCT?

131. Todd Bishop, *Clarke Rips Microsoft over Security*, SEATTLE POST-INTELLIGENCER, Feb. 17, 2005, *available at* http://seattlepi.nwsource.com/business/212437_rsaclarke17.html.

132. *Id.*

133. For a discussion on the unknown weights of the factors that need to be considered to make good policy in this area, see Bruce Berkowitz & Robert W. Hahn, *Cybersecurity: Who's Watching the Store?*, ISSUES IN SCI. & TECH., Spring 2003, at 55.

134. An in-depth discussion of the political feasibility of expanding tort liability to Microsoft or software in general is beyond the scope of this Note.

To bring a products liability suit against Microsoft, it must first be established that Windows is a product.[135] *The Restatement (Third) of Torts: Products Liability* defines a product as "tangible personal property distributed commercially for use or consumption."[136] Items such as real property and electricity are also products when their use and context are "sufficiently analogous" to other cases involving conventional products.[137]

When dealing with classifications of software, the debate often focuses on whether software is a "good" under the U.C.C., and many courts have opted to say yes, consequently applying the U.C.C.'s Article 2 on the sale of goods.[138] When software is custom-made to fit the needs of a business, some courts have classified it as a service and applied the common law rules of negligence and contracts.[139] Sometimes, courts must determine whether the contract between the software vendor and buyer predominantly included services or a sale of goods in order to determine whether to apply common law rules or the U.C.C.[140]

The U.C.C. defines goods as all things that are "movable at the time of identification to the contract for sale."[141] The uncertainty about the applicability of the U.C.C. arises because software, though sold in discrete packages, is often accompanied by licensing agreements that retain intellectual property rights in the software company and control the user's discretionary use of the product.

Not all courts find the distinction meaningful. In *ProCD v. Zeidenberg*, the court dispensed with an analysis of the categorization of software, stating that it will "treat the licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code. Whether

135. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19(a) (1998).

136. *Id.*

137. *Id.*

138. *E.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996) (finding that licenses are "ordinary contracts"); Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 676 (3d Cir. 1991) (finding that computer software is a good within the U.C.C. and noting that application of the U.C.C. to software will offer uniform laws to analyze implied warranties, consequential damages, and disclaimers of liability). *See generally* RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 6:4 (2005) (discussing whether computer-related transactions are goods or services).

139. *E.g.*, Micro-Managers, Inc. v. Gregory, 434 N.W.2d 97, 100 (Wis. Ct. App. 1988) (finding that the contract for customized software was primarily a service contract based upon terms in the contract, such as "man-days," "development," and "time," and the use of labor costs as the predominant method of billing).

140. *See Advent Sys. Ltd.*, 925 F.2d at 675–76.

141. U.C.C. § 2-105 (2000).

there are legal differences between 'contracts' and 'licenses' . . . is a subject for another day."[142] Here, the issue was whether software licenses are binding on the user. The court applied the U.C.C. rules on acceptance of a contract to bind the consumer to a license that appeared on a splash screen.[143] The court's decision was driven by the desire to promote the freedom of contract.[144] The court believed that terms of a license and warranty were strategic areas in which software vendors should compete with one another without the interference of the judiciary.[145]

Sometimes, this distinction is crucial in identifying each party's rights. Courts have focused on the ownership rights created by a license when it protects vendors' intellectual property rights and allows them to engage in price discrimination among its various consumers. [146] Citing *Adobe Systems Inc. v. One Stop Micro, Inc.*, the court in *Adobe Systems Inc. v. Stargate Software Inc.*, treated the transaction between the consumer and Adobe as a licensing agreement.[147] Specifically, the court distinguished between the user's ownership of the medium, the CD, and the licensor's ownership of the content of the CD, the software.[148] By doing so, the court protected Adobe's right to restrict the distribution of software to the terms provided in the licensing agreement.[149]

In contrast, in *Softman Products Co. v. Adobe Systems, Inc.*, a California district court found that Adobe sold its software as a good, not under a license for use.[150] The court explained, "'If a transaction involves a single payment giving the buyer an unlimited period in which it has a right to possession, the transaction is a sale.'"[151] All three Adobe cases dealt with substantially similar software and licensing terms, yet resulted in two

142. *ProCD*, 86 F.3d at 1450.

143. *Id.* at 1452–53.

144. See *id.* at 1453.

145. *Id.*

146. *See* Adobe Sys. Inc. v. Stargate Software Inc., 216 F. Supp. 2d 1051, 1059 (N.D. Cal. 2002); Adobe Sys. Inc. v. One Stop Micro, Inc., 84 F. Supp. 2d 1086, 1092 (N.D. Cal. 2000).

147. *See Stargate Software Inc.*, 216 F. Supp. 2d at 1056–60.

148. *Id.* at 1055.

149. *Id.* at 1059.

150. *See* Softman Prods. Co. v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1084 (C.D. Cal. 2001). This court in turn had rejected the holding in *One Stop Micro, Inc.*, 84 F. Supp. 2d at 1091, that the transaction in issue is a license. *Softman Products*, 171 F. Supp. 2d at 1086–87. The *One Stop Micro* court relied upon Adobe's assertion that licensing was the favored method of distribution of software. *One Stop Micro*, 84 F. Supp. 2d at 1091–92. The Stargate court adopted the One Stop court's analysis. *Stargate Software*, 216 F. Supp. 2d at 1056.

151. *Softman Products*, 171 F. Supp. 2d at 1086 (quoting RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 1:18 (1992)).

divergent analyses.

The developing case law is inconsistent and incoherent at best. Professor Nimmer notes that this debate results from the inadequacy of the existing classifications.[152] He states that information is neither a good nor a service and that courts should not artificially apply the U.C.C.[153] He laments that courts do not force the application of the implied warranty of merchantability to the text of a book, but sometimes apply it to software.[154] Nimmer concludes that the common law of contracts is the most appropriate body of law for analyzing transactions between vendors and consumers, because the distribution occurs under a license, not a sale.[155]

In response to this emerging hodgepodge, the revised U.C.C. explicitly excludes "information" from the definition of "goods."[156] Instead, information transactions are addressed in the new Uniform Computer Information Transaction Act ("UCITA").[157] At the time of writing, no states had adopted the revised U.C.C.,[158] and only Maryland and Virginia had adopted UCITA.[159]

Notwithstanding the differences in software and other goods, the courts apply the U.C.C. for a reason. It may be that Article 2 provides an easy analysis.[160] It may stem from the intuitive, consumer perception that one buys software as an enabling tool for productivity or entertainment, not as a source of information. The software designer designs programs to interact seamlessly with the user and fiercely protects the source code. The average consumer does not care to know about the source code, but expects a computerized tool to perform specific tasks. Specifically, an operating system is expected to manage the input from the user and the applications that run on the computer. The manner in which consumers use the "information" that they paid for differs dramatically from the way in which they use information from a book. The information operates a tool, which

152. NIMMER, *supra* note 138, § 6:4, 6-7–6-8.

153. *Id.* § 6:4, 6-8.

154. *Id.*

155. *Id.*

156. U.C.C. § 2-103(k) (2003).

157. U.C.I.T.A. (2002). Professor Nimmer was on the committee that drafted UCITA. *Id.*

158. Nat'l Conference of Comm'rs on Unif. State Laws, A Few Facts About the Amendments to UCC Articles 2 and 2A, http://www.nccusl.org/Update/uniformact_factsheets/ uniformacts-fs-UCC22A03.asp (last visited May 26, 2007).

159. Nat'l Conference of Comm'rs on Unif. State Laws, A Few Facts About the Uniform Computer Information Transactions Act, *at* http://www.nccusl.org/Update/uniformact_ factsheets/uniformacts-fs-ucita.asp (last visited May 26, 2007).

160. NIMMER, *supra* note 138, § 6:4, at 6-11.

has replaced many mechanical counterparts such as typewriters, drafting tables, calculators, and so on. The drafters of UCITA acknowledged this and created three implied warranties of merchantability: one for a computer program,[161] one for informational content,[162] and one for licensee's purpose/system integration.[163]

For purposes of analysis, the status of software as a good determines how the courts analyze the contractual warranties and disclaimers under the license. If UCITA is uniformly adopted, liability would be virtually impossible to impose on software companies.[164] For purposes of ultimate liability, however, whether software is licensed or sold, it is commercially distributed for use and is "sufficiently analogous" to other products to be subject to products liability.[165] The purpose of Microsoft's license, much like the licenses in the Adobe cases, is to protect Microsoft's profits through a contract that limits distribution, prevents alteration, and retains title to the intellectual property.[166] The use of a license, therefore, does not preclude the use of products liability or similar law.

B. THE U.C.C. ANALYSIS

If software is considered a good under the U.C.C., a plaintiff must overcome the warranty disclaimers. The U.C.C. assumes that parties bargained for the terms of sale and that market competition will protect consumers.[167] Therefore, though it provides consumers with an implied warranty of merchantability,[168] it also allows sellers to disclaim these warranties as long as they are conspicuous[169] and to limit remedies on any

161. U.C.I.T.A. § 403 (2002).

162. *Id.* § 404.

163. *Id.* § 405.

164. UCITA permits the disclaimer of the implied warranty of merchantability for computer programs. *Id.* § 406.

165. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19(a) (1998) (allowing items such as real property and electricity to be considered 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").

166. *See* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 96 n.7 (3d Cir. 1991) (detailing the development of the software license as a way to avoid the first sale doctrine of copyright law, which allows anyone who buys a copyrighted work to sell or lease it to others).

167. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996). Judge Easterbrook notes that the terms of use of a software license are "no less a part of 'the product'" than the software itself. *Id.* Market forces protect the consumer by electing to compete by offering "improved terms of use" among other things. *Id.*

168. U.C.C. § 2-314 (2000).

169. *Id.* § 2-316(2).

undisclaimed warranties.[170] In theory, as Judge Easterbrook noted in *ProCD*, the price of the product includes the strength of the warranty.[171]

UCITA also allows the disclaimer of the implied warranty of computer programs.[172] The implied warranty warrants "to its end user licensee that the computer program is fit for the ordinary purposes" of its use.[173] Comment 3(a) clarifies that to be "fit," a program must be within the "average levels of quality and reasonable standards of program capability" which will inevitably be redefined over time and be less than perfection.[174] But, if Microsoft dominates the operating systems market, is it not by definition the benchmark for average?

Shrinkwrap agreements usually disclaim all warranties, limit liability, and limit the remedy available to the consumer to the price of the software.[175] The End-User License Agreement ("EULA") for Microsoft Windows XP Professional provides a limited warranty for only ninety days for products acquired in the United States or Canada that the "[p]roduct will perform substantially in accordance with the accompanying materials."[176] Any statutorily imposed implied warranty that can be disclaimed after these ninety days is fully disclaimed.[177] Even this limited warranty is void if the product's failure results from a virus.[178] The EULA further disclaims all possible warranties and conditions of merchantability[179] and excludes incidental, consequential, punitive, and indirect damages, even in the "event of the fault, tort (including negligence), strict liability, breach of contract or breach of warranty of Microsoft or any supplier, and even if Microsoft or any supplier has been

170. *Id.* § 2-719.

171. *See ProCD*, 86 F.3d at 1453.

172. U.C.I.T.A. § 406 (2002).

173. *Id.* § 403 (a)(1).

174. *Id.* § 403 cmt. 3(a).

175. *See* Steven P. Mandell & Stephen J. Rosenfeld, *Drafting Software And Trademark Licenses For Litigation*, *in* 845 PRAC. L. INST., PATENTS, COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES 795, 802-03, 812 (2005). Shrinkwrap or clickwrap agreements are the agreements that accompany software. *See, e.g.*, *ProCD*, 86 F.3d at 1449, 1452 (explaining shrinkwrap agreements and discussing a clickwrap agreement entered into where the license terms were "splashed" across a computer screen and acceptance had to be indicated in order to continue).

176. MICROSOFT CORP., MICROSOFT WINDOWS XP PROFESSIONAL END-USER LICENSE AGREEMENT § 11 (July, 27, 2001), *at* http://download.microsoft.com/documents/useterms/Windows%20XP_Professional_English_9e8a2f82-c320-4301-869f-839a853868a1.pdf [hereinafter, MICROSOFT EULA].

177. *Id.*

178. *Id.*

179. *Id.* § 12.

advised of the possibility of such damages."[180]

As long as courts uphold these agreements, Microsoft and other software manufacturers may contract away their liability. The U.C.C. and contract law allow this as long as the contract or the clause is not unconscionable.[181] The licensor typically wins.[182]

In software cases, procedural unconscionability can easily be avoided by using larger print, all caps, or other typeface modifications to emphasize any limitations on liability.[183] The use of splash screens where the user can click "I Agree" to accept the licensing agreements has been upheld in *ProCD*[184] and endorsed by the drafters of UCITA.[185]

Licenses routinely provide the minimal remedy to avoid unconscionablilty of terms.[186] The Microsoft EULA's general limitation on remedies gives consumers the greater of the price paid for the product or five dollars.[187] Yet, another copy of the operating system would inevitably include an identical flaw, making a product exchange meaningless unless the CD itself is damaged. Many consumers likely cannot function without Windows due to its virtual monopoly, so a full refund with the return of the product is a meaningless remedy. A consumer who opts to use Linux or Apple's operating system risks incompatibility with other software bundles and network configurations.

The continued use of arguably unconscionable terms that limit liability and remedies in software contracts should not be viewed as evidence of their enduring usefulness. Rather, they may be viewed as a "no-lose gamble" for the software manufacturer.[188] Unless a consumer contests the carefully drafted terms, the software manufacturer may seek to enforce them. By disclaiming all warranties and providing the minimum remedy

180. *Id.* § 13 (all caps removed).

181. U.C.C. § 2-302 (2000); RESTATEMENT (SECOND) OF CONTRACTS § 208 (1979). *See also* Mandell & Rosenfeld, *supra* note 175, at 805. The U.C.C. comment says that the "principle is one of the prevention of oppression and unfair surprise . . . and not of disturbance of allocation of risks because of superior bargaining power." U.C.C. § 2-302 cmt. 1 (2000). Despite this comment, Professor Slawson notes that the U.C.C. purposely leaves the term "unconscionable" vague to allow courts to include "protection against abuses of superior bargaining power" under unconscionability in order to uphold the principles that underlie it. SLAWSON, *supra* note 122, at 142.

182. Mandell & Rosenfeld, *supra* note 175, at 805.

183. *Id.* at 805–06.

184. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452–53 (7th Cir. 1996).

185. U.C.I.T.A. § 112 cmt. 5, illus.1-3 (2002).

186. *See* Mandell & Rosenfeld, *supra* note 175, at 807, 812.

187. MICROSOFT EULA, *supra* note 176, § 15.

188. SLAWSON, *supra* note 122, at 143.

required to overcome unconscionability as a matter of law, software manufacturers have effectively found the "slickest 'get out of jail free card.'"[189]

The *ProCD* court's assumption that an improved license or warranty would provide a basis for competition appears to be undercut by the exclusive role of licenses in reducing litigation for software vendors.[190] As noted by Professor Rustad, "One can read hundreds of click-wrap . . . and other mass-market transactions and have yet to find a single example of a software licensor willing to provide any warranty for its software."[191] In the case of Microsoft, because very few consumers can forgo the use of Windows, a court may find that this EULA is an unconscionable agreement because of Microsoft's extraordinarily superior bargaining power.

The utter uselessness of computer warranties to the consumer (or effectiveness for the manufacturer) suggests that if liability via tort law fails, legislation can impose a mandatory minimum warranty for security instead.

D. THE DESIGN DEFECT

Assuming that the plaintiff is able to overcome the barriers posed by the warranty, under a products liability theory, the design defect should be defined as the inability of the operating system to keep data secure and safe from unauthorized access.

If, however, the claimed design defect is Microsoft's integration of products as claimed by the report published by the Computer and Communications Industry Association,[192] the plaintiff will likely lose. Microsoft will undoubtedly argue that the integration of its products through its operating system is the very feature that catapulted Windows to its position of dominance. Thus the utility and productivity resulting from this product integration far outweigh any risks. Given the complexity of building an operating system, showing a reasonable alternative to the court—in other words, designing a new operating system—would be a near impossible task. Despite the compelling argument that Microsoft's product integration is an inherent security risk, courts are ill-equipped to solve this

189. McCullagh, *supra* note 117 (quoting Richard Forno, security expert).

190. *See* Mandell & Rosenfeld, *supra* note 175, at 802–21 (explaining how to draft software licenses to hold up in court while shielding software vendors from liability).

191. Michael L. Rustad, *Making UCITA More Consumer-Friendly*, 18 J. MARSHALL J. COMPUTER & INFO. L. 547, 579 (1999).

192. *See supra* text accompanying notes 68–70.

problem.

Alternatively, if there is a mandated express warranty for security, plaintiffs must show that the goods failed to function as warranted.[193] Evidence of a security failure caused by a Microsoft bug would be sufficient to show a breach of warranty.

E. CAUSATION AND PROXIMATE CAUSE

Causation of the security breach and consequential harm may be easily shown. An expert can explain how a programming error or a feature allowed a security breach to occur. Institutions such as CERT and the antivirus company Symantec track malicious code and their signatures.[194]

Proximate cause of a security breach, however, will be a thorny issue, especially in the case of identity theft of a home user. In 2003, only fifty-one percent of victims of identity theft knew how their identity was stolen.[195] Even if consumers are aware of unauthorized access to their computer data, proving that their identity theft came from a security flaw on the computer and not from a lost wallet, stolen mail, or a friend requires omniscience. Unfortunately, the reality of what may be known may trump any theory of tort liability in this realm. It is possible that some forms of misappropriation will be traceable through circumstantial evidence, but these cases may be rare. As more data becomes available about cyber identity theft, the effect of proximate cause on claims will become clearer.

F. ECONOMIC LOSS DOCTRINE PRECLUDES RECOVERY

Under the current law, in the unlikely instance that the plaintiff successfully moves her case out of contract theory and into tort and successfully argues a design defect theory of liability, she will still be foiled by the economic loss doctrine. A plaintiff may easily be able to show that the operating system had insufficient mechanisms for security but may not be able to demonstrate any recoverable damage. The most common injuries in a cybersecurity case will be the loss of data, financial harm,

193. 3 LARY LAWRENCE, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 2-313:191 (3d ed. 2002).

194 *See* Tom Zeller, Jr., *Cyberthieves Silently Copy Your Passwords as You Type*, N.Y.TIMES.COM, Feb. 27, 2006, *available at* http://www.nytimes.com/2006/02/27/technology/27hack.html; CERT RESEARCH, 2005 ANNUAL REPORT 4 (2006), *at* http://www.cert.org/archive/pdf/cert_rsrch_annual_rpt_2005.pdf.

195. *See* SYNOVATE, FED. TRADE COMM'N, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 30 (2003), *available at* http://www.consumer.gov/idtheft/pdf/synovate_report.pdf.

dignitary injury, and an invasion of privacy[196]—all damages that cannot be characterized as physical injuries or damage to "other property." Essentially, the economic loss doctrine wipes away all liability, unless the courts create an exception for public policy reasons.

G. APPLICATION OF THE ECONOMIC LOSS DOCTRINE IN THREE TYPES OF CYBER ATTACKS

1. Deletion of Files

Fundamentally, the economic loss doctrine addresses the need to limit tort liability to those harms that "implicate the liberty and integrity of the person."[197] Damages to personal property are recoverable because "personal property is . . . bound up with the social realization of personhood."[198] We are now in the Information Age, and our lives are bound up in data.[199] The problem of characterization exists because we do not technically own data as property, though a lively debate is ongoing as to whether we should.[200] Yet, it remains undeniable that the fruits of our labor are increasingly being created in data and data compilations. The value of data provides persuasive support for creating limited property rights in data.

The economic loss doctrine may also be justified as a way to maintain economic efficiency.[201] When there is physical damage there is a permanent, net loss to society.[202] In contrast, when only economic damages

196. Rustad & Koenig, *supra* note 37, at 1603.

197. Gregory C. Keating, *Reasonableness and Rationality in Negligence Theory*, 48 STAN. L. REV. 311, 344 (1996).

198. *Id.*; Anita Bernstein, *Product Dynamism and the Law, in MEANING, MEASURE, AND MORALITY OF MATERIALISM (Floyd Rudmin & Marsha Richins eds., 1992), in* A PRODUCTS LIABILITY ANTHOLOGY, 177, 179–80 (Anita Bernstein ed., 1995).

199. Loss of data strikes some as a "life-changing problem" when a user stores all of his data on his computer, such as tax returns, photos, and creative work without backing them up. Conrad Mulcahy, *The Errors Are Fatal, but Maybe There's Hope*, N.Y.TIMES.COM, Mar. 21, 2006, *available at* http://www.nytimes.com/2006/03/21/nyregion/21ink.html.

200. *See generally* Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135 (2004) (noting that real property rights have never been absolute and discussing the bundle of rights and responsibilities that might constitute information property); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (providing one way to commodify data while balancing information privacy concerns and the market value of compiling personal information).

201. *See* Daniel London, *Is the Economic Loss Rule in Peril? Courts, Negligence and the Economic Loss Wolves*, 71 DEF. COUNS. J. 379, 382–83 (2004).

202. *Id.* at 382.

arise, the loss results in a shift of resources.[203] In the case of businesses, the loss in profits for one business may be a windfall for another.[204] By barring recovery for pure economic loss, the law allows the market to strike a new balance from the shift in financial advantage.

The economic loss doctrine may also be seen as a simple way to limit damages from a products liability case.[205] Products liability is a policy driven imposition of liability. No court wants to put Microsoft out of business by straddling it with infinite damages that it cannot control. In the seminal economic loss case, *East River Steamship Corp., v. TransAmerica Delaval, Inc.*, the United States Supreme Court determined that "[i]n products-liability law, where there is a duty to the public generally," the use of the economic loss doctrine was favored over the use of a foreseeability test because compensating for all foreseeable economic loss would result in vast liability.[206] In that case, plaintiffs claimed economic damages against a turbine designer and manufacturer, where a defective turbine damaged itself while in operation.[207] The Court denied recovery, finding that an action in warranty was appropriate when the property damaged is covered under the contract for sale[208] and stressed the need to keep tort and contract law in separate spheres.[209]

More recently, loss of data has been found to fall under pure economic loss. In *Transport Corp. v. IBM*, the court followed the same analysis as *East River Steamship* and found that the data stored on a hard disk drive was integrated into the computer system.[210] Therefore, when the hard disk failed, taking the data with it, the cost of the data was irrecoverable as economic loss.[211] Moreover, because Transport Corporation backed up its data daily, the court found that it was aware that the hard disk may fail.[212] Under Minnesota tort law, Transport Corporation could not recover for any product defects that could "ordinarily be contemplated"[213] under the

203. *Id.*
204. *Id.*
205. *See* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 866–67 (1986); R. Thomas Cane & Sheila Sullivan, *The Future of the Economic Loss Doctrine in Wisconsin*, 78-May WIS. L. 12, 13 (2005).
206. *E. River S.S. Corp.*, 476 U.S. at 874.
207. *Id.* at 859, 867.
208. *Id.* at 868.
209. *Id.* at 871.
210. Transp. Corp. of Am. v. Int'l Bus. Machs. Corp., 30 F.3d 953, 957 (8th Cir. 1994).
211. *See id.*
212. *Id.* at 958.
213. *Id.*

contract. Arguably, the *Transport* court reached the correct result because the purpose of a hard drive is to store data, and its failure should be covered under the contract for sale. Similarly, in *Rockport Pharmacy, Inc. v. Digital Simplistics*[214] and *Fidelity Deposits v. IBM*,[215] the courts found that the loss of data was pure economic loss, not "other property" that was separate from the computer that failed. The *Fidelity* court found that data are not tangibly separate from a computer, noted that the plaintiff failed to supply an adequate definition or description of data as other property, and ultimately based its decision on its concern that the problems of valuation and proof surrounding lost data could lead to endless litigation.[216]

Insurance cases have similarly dealt with the issue of data recovery under general liability policies that covered only loss to "tangible" property. These cases deal with contract interpretation but are nevertheless instructive. Prior to the creation of stand-alone cyberinsurance policies, companies with general commercial liability policies attempted to claim damages to data as a covered loss.[217] In *American Guarantee and Liability Insurance Co. v. Ingram Micro, Inc.*, a federal district court interpreted an insurance contract covering "physical" damage.[218] The court found that physical damage to a computer was not limited to the destruction of computer circuitry but also included the loss of access, use, and functionality to the computer.[219] The court looked to criminal statutes that defined damage in computer-related cases to justify its broad interpretation of "physical."[220] This holding caused tremors in the insurance community.[221] Critics noted that courts have traditionally drawn the line for coverage, differentiating between the value of the destroyed media (covered) and coverage for the value of the ideas (not covered).[222]

These cases highlight two conceptual problems. The first is whether

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

215. *See* Fid. & Deposit Co. of Md. v. Int'l Bus. Machs. Corp., 2005 WL 2665326, at *3 (M.D. Pa. Oct. 19, 2005).

216. *Id.*

217. Paula M. Yost, Paul E.B. Glad & William T. Barker, *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Computer Data*, 54 SMU L. REV. 2055, 2056 (2001).

218. Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., 2000 WL 726789, at *2 (D. Ariz. April 18, 2000).

219. *Id.* at *2.

220. *Id.* at *2–3.

221. *See* Yost, Glad & Barker, *supra* note 217, at 2056–57.

222. *Id*. at 2057. *See, e.g.*, Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp.2d 459, 468 (E.D. Va. 2002), *aff'd*, 347 F.3d 89, 98 (4th Cir. 2003) (holding that data is not tangible property).

data are property at all.[223] The second problem arises when data are considered generally integrated into the computer. Presumably, an operating system would be considered integrated into the same computer with the data. But there are salient differences. Though one may contemplate the loss of data from a hard drive failure and shop for warranties and quality accordingly, one probably does not equally contemplate the loss of data from the choice of operating system. Treating the data, the operating system, and the computer as one entity, because it looks like one box, creates more conceptual problems than evaluating each piece in relation to the other. To illustrate this point, consider products liability cases that involve large products made up of smaller components. In *Jimenez v. Superior Court*, the California Supreme Court reaffirmed that in California "the economic loss rule does not necessarily bar recovery in tort for damage that a defective product . . . causes to other portions of a larger product . . . into which the former has been incorporated."[224] Following this rule, they held that a manufacturer of defective windows for a mass-produced home can be held strictly liable for harm to other parts of the home.[225] A similar analogy can be made to a defective operating system in relation to data.

Furthermore, data do not have to be considered part of a whole product at all. When a CD goes into a CD player, the CD is not integrated into the player because it is removable. Why then does it become integrated into the computer and lose all value if the contents are copied onto a hard drive? Allowing recovery for lost data does not compromise the doctrinal rationales behind the economic loss doctrine: protecting things that give meaning to our personhood and compensating for a true loss.

Assuming that highly sophisticated individuals will back up data that they cannot afford to lose, the actual liability exposure may be quite small. Of course, it may be quite large depending on users' back up habits. This problem of a heterogeneous customer pool is discussed below.[226]

Ultimately, despite the plausible policy arguments for considering data as property for purposes of the economic loss rule, courts may find that the loss of information is not recoverable. Given the case law, a substantial change in conceptualization of data would be required. Whether the court's interpretation of "physical" damage to computers in *American Guarantee*

223. *See supra* text accompanying notes 198–200.
224. Jimenez v. Superior Court, 58 P.3d 450, 457 (Cal. 2002).
225. *Id.*
226. *See infra* Part V.

gains traction remains to be seen.

2. Misappropriation of Data

Recently, Symantec reported that half of the malicious code it tracks is designed to gather personal data rather than inflict harm on the network or other computers.[227] The criminal hacking statute's inclusion of "impairment to the integrity . . . of data" in the definition of "damages" underscores the reality that unauthorized use of data constitutes damage when dealing with data.[228] Statutes such as the Gramm-Leach-Bliley Act impose duties upon financial institutions to safeguard financial data of customers.[229] But imposing liability on Microsoft for the misappropriation of data from personal computers presents a difficult analysis.

Under a strict application of the economic loss doctrine, no recoverable damage has occurred. Assume for the moment, however, that due to the heightened concern for privacy and fraud prevention, the law creates an exception for data theft caused by a security flaw. The rationale for shifting risk remains the same. Microsoft has control over the code. The key to preventing unauthorized access is in Microsoft's hands.

When a home user falls victim to identity theft, for example, calculable damages exist. If not, damages may be any out-of-pocket costs to monitor financial activity.[230] These are concrete damages that are easily quantifiable. Under products liability law, however, the law must create an exception to the economic loss doctrine to permit this recovery.

3. Denial of Service

Any downtime from a denial of service attack that debilitates a computer network would be a pure economic loss and not recoverable. Though a denial of service attack undeniably results in loss of productivity, it is akin to lost profits from an electricity outage[231] or lost productivity

227. *See* Zeller, Jr., *supra* note 194.

228. 18 U.S.C. § 1030(e)(8) (Supp. 2002).

229. 15 U.S.C. § 6801(b) (2000).

230. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 307–08 (2005). Johnson advocates imposing tort liability onto data processors for inadequate cybersecurity, while also cautioning against imposing unlimited liability. *Id.* at 311. He favors capping damages to out-of-pocket costs of monitoring security and taking reasonable steps to prevent future identity theft. *Id.* at 307–08.

231. *See* FMR Corp. v. Boston Edison Co., 613 N.E.2d 902, 903 (Mass. 1993) (holding that the loss of income and increase of costs to an investment firm from a power outage is not recoverable under the economic loss doctrine).

from sitting idle on a bridge waiting for a car accident to clear.[232]

Furthermore, a Slammer-like attack that may render all of South Korea's cell phone and Internet systems unusable would subject Microsoft to ruinous liability. Despite the security flaws, Microsoft's products are undisputedly beneficial tools in our modern lives, and the law needs to shield it from this type of a calamity.

And yet, the greatest fear when dealing with cybersecurity is this very one: the catastrophic failure of critical infrastructure when a software bug wreaks havoc on the networked system.[233] Why should Microsoft escape liability? Tort law is not only about compensating victims but also about balancing competing interests of innovation and safety. Furthermore, the underlying flaw that creates liability for loss of data or identity theft will be the same flaw that creates cataclysmic disaster. Therefore imposing tort liability for improbable catastrophes does not further any policy goals that are not already addressed, while taxing Microsoft at a level that exceeds any societal benefit.

V. ALTERNATIVE SOLUTIONS ROOTED IN CONTRACTS

A. MANDATORY WARRANTY

In evaluating potential liability for Microsoft, the critical issue is the scope of liability, which products liability law addresses by flatly denying recovery via the economic loss doctrine. By unpacking the problem, a different solution emerges. Microsoft controls the code. Hackers control the nature of the harm. Users control the extent of the harm because they control how they use their computers.[234] These variables span an unpredictable range that Microsoft is not in a superior position to predict. In a perfect world, Microsoft should be able to efficiently distribute the loss among its consumers and provide insurance for its consumers by pricing its products appropriately.

232. *See* KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 234–35 (2d ed. 2002).

233. In the late 1990s, the Pentagon and the media believed that an "Electronic Pearl Harbor" at the hands of terrorists was imminent, a threat that never materialized. George Smith, *An Electronic Pearl Harbor? Not Likely*, ISSUES IN SCI. & TECH., Fall 1998, at 68.

234. Professors Lichtman and Posner note that Microsoft could require that its users update its software on a regular basis via its licensing agreements, thus shifting the control over security updates back to Microsoft from consumers. Lichtman & Posner, *supra* note 54, at 236. This solution, however, would not change any risky behavior by users that may expose them to malicious code.

Commercial cyberinsurance providers tie insurance rates to an ex ante evaluation of the business's security procedures,[235] providing discounts to businesses that install professional security systems,[236] and charging more for businesses that rely on computing.[237] Premium prices still remain high, and cyberinsurance companies do not have enough data about computer failures, network attacks, and the extent of resulting damages to accurately calculate risk and set prices accordingly.[238] Yet they solved the problem of uncertain risk by requiring evaluations. If exposed to liability, Microsoft faces a great problem because it cannot tie recovery to ex ante evaluations of its customers' behavior; it can only encourage its customers to adopt less risky behavior. On the other hand, the diversity of consumers exposes Microsoft to the average risk; insurance companies face the problem of attracting a pool of high risk customers.[239] Among all of the uncertain variables that require more research, one variable, liability, can be capped, much the same way that insurance providers cap coverage.

In the end, a potential solution requires circling back to the inadequate warranty provided by software companies for security failures. If liability is necessary to effectuate policy goals, the easiest solution may be to restrict software vendors' ability to disclaim liability, while capping damages to a predetermined amount. Essentially, when consumers purchase a Microsoft operating system, they will also purchase a form of mandatory insurance against cyberattack. Instead of paying for cybersecurity with out-of-pocket costs, they will be paying for it in the form of a warranty.

To be effective, the warranty must cover the damage caused by a security flaw. Presently, the limited warranty provided by Microsoft provides a refund or a replacement with a return of the product, though not for failures caused by a virus.[240] Given Microsoft's virtual monopoly on the market, this limited remedy for a security breach renders the warranty meaningless. The remedy must include some consequential damages.[241]

Furthermore, with a mandatory warranty, plaintiffs may file for a

235. Kesan, Majuca & Yurcik, *supra* note 96, at 27–28.

236. *Id.* at 28.

237. *Id.* at 27–28.

238. *Id.* at 29.

239. *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. OF ECON., 488, 492–94 (1970) (illustrating that when the pool of customers for insurance is made up of high-risk individuals, no amount of insurance can be bought for any price).

240. MICROSOFT EULA, *supra* note 176, §§ 11, 13.

241. Consequential damages are defined in U.C.C. § 2-715 (2000) and include "injury to person or property proximately resulting from any breach of warranty." *Id.*

breach of express warranty claim if it is not honored. A breach of warranty claim permits recovery for economic losses.[242] This avoids the endless conceptual roadblocks presented by products liability, a rule rooted in tangible products that cause visible harm. It also prevents the creation of convoluted case law that may result from reconceptualizing data and carving out exceptions to the economic loss doctrine.

Showing that Microsoft's products caused the harm in question will remain a difficult task. To ward off frivolous claims, Microsoft would and should promulgate clear standards for evaluating whether a warranty claim is valid. Due to the latent nature of the defect and the difficulties in tracing the cause of the damage, this may present a high bar for many victims. Unlike a products liability suit, however, the clearer cases have a chance for recovery without cumbersome and costly litigation.

Quantifying the harm continues to pose a problem. For example, a denial of service attack that floods the network and affects home users in unpredictable ways may have unquantifiable harms. In crafting the warranty, care must be taken to address this issue. Insurance plans fail when there is a high probability of harm to a large number of customers at the same time.[243] Since this warranty is a form of insurance, forcing Microsoft to cover the cost of unquantifiable damage that may occur on a large scale is unreasonable. Damage to data may also be hard to quantify, but a more concrete pricing scheme can be designed based on what types of data were lost or how much data were lost.

Care should also be taken in setting the maximum cap for recovery under the warranty. If the warranty is mandatory and imposed on Microsoft, we must be concerned about appropriately drawing the line for damages. The ubiquity and reach of the Internet created the risk of cyber attacks and the need for liability; yet, precisely the same reason dictates that damages need to be limited in a reasonable manner. Data from the cyberinsurance market for business users may provide some insight in setting a number. Alternatively, a temporary cap can be created, for example, $10,000 per license, and revisited every two years or so for re-evaluation.

B. MITIGATION: CONSUMERS

Finally, consumers must also shoulder the burden of an increasingly

242. LAWRENCE, *supra* note 193, § 2-314:114.

243. Mehr, Cammack & Rose, *supra* note 113, at 730–31.

unsafe cyber world. Much as a city dweller would never leave the front door unlocked, a cyber dweller should never leave the door wide open for malicious code.

Therefore, the consumer's conduct in maintaining reasonable security should be considered. Arguably, Microsoft should not be selling products with any security flaws and should continue to be held liable even if it does disseminate a patch. This approach, however, improperly penalizes Microsoft for its efforts. Notably, any cyberinsurance recovery is predicated on security maintenance, providing an incentive for many businesses to maintain a high level of care. Home consumers should similarly be responsible for maintaining a reasonable level of security to recover under warranty. The word "reasonable" is critical because as technology changes and Microsoft integrates its security updates to its newer products, different standards will apply. Consumers will also differ in their ability to access patches and updates, as not all consumers have an always-on broadband connection.

This policy also encourages Microsoft to continue to improve their Windows update service that delivers security updates to home computers.

VI. CONCLUSION

Given the increased reliance on computing and the need for security for all users, the costs of security flaws, especially for operating systems, should no longer be externalized and borne by the users. The review of the developing case law suggests that the use of products liability law will require both an invalidation of the current warranty disclaimer that is used by Microsoft and the creation of an exception to the economic loss rule for computer-related losses. As more software becomes available via subscription with continuous upgrading, courts may become less inclined to describe software as a product, though the preferred distribution model for mass-retail software remains to be seen.[244] Products liability law is an intuitive solution to a problem that stems from a product placed in the stream of commerce but requires substantial changes in perspectives and attitudes of the courts.

244. *See, e.g.*, FREDERICK CHONG & GIANPAOLO CARRARO, MICROSOFT CORP., ARCHITECTURE STRATEGIES FOR CATCHING THE LONG TAIL (Apr. 2006), *at* http://msdn2.microsoft.com/en-us/library/aa479069.aspx. This Microsoft article explains how "software as a service" works, including how delivering software as a service may require a shift in how software vendors think about software ownership and their existing business models. *Id.*

Alternatively, the underlying problem may be solved by disallowing warranties that disclaim all liability for security. If the law mandated that Microsoft provide a warranty for the security of its products for home users, the same policy goals that drive the desire to impose tort liability on Microsoft would be served, while appropriately limiting liability. Microsoft will continue to improve the security of its products both to reduce any warranty claims and to keep prices down for consumers. As the risk of a security flaw decreases, Microsoft can lower the price it must charge consumers for the mandated warranty. Consumers will have a better avenue for recovery, especially on smaller claims that would otherwise require resorting to a class action lawsuit.

The need for security does not end with Microsoft. Its dominance in the computing world presented an opportunity to explore the ramifications of liability in a more concrete manner for the purposes of this Note. If Microsoft is held liable for its flaws, the liability for other software vendors would similarly follow. This Note assumes that consumers prefer a warranty for security rather than cheaper software. If this is true and a mandatory warranty is created, it would have implications for not only established giants such as Microsoft, but also the distribution and pricing mechanisms for open source software.[245] The ultimate unanswered question is: How much is the security of our personal data actually worth? Is the security of our data worth so much that we should not be able to contract it away?

245. Redhat, the largest retailer of Linux, provides the operating system for free but charges for a subscription service for patches, updates, and technical support. Other business models for making money with free, open source software are discussed by the Open Source Initiative. Open Source Initiative, Open Source Case for Business (Mar. 31, 2007), *at* http://www.opensource.org/advocacy/case_for_business.php. The open source revolution depends upon the ability of the programmers to disclaim all warranties and liabilities. See Open Source Initiative, The Approved Licenses (Sept. 19, 2006), *at* http://opensource.org/licenses for samples of approved licenses that detail how rights and responsibilities are allocated.