Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?

Robin A. Brooks

Table of Contents

> "The chance that a law will achieve its intended purpose improves when it is grounded in an accurate understanding of the phenomena it will regulate."[1]

I. Introduction

Damages caused by malicious software code will likely result in increasing civil tort litigation, considering the phenomenal growth of the electronic business paradigm and communications over the Internet.[2] The potential for personal injuries increases as more computer software controls systems with which people come into contact.[3] Successfully managing this growth portends a balance of

---

1. Pamela Samuelson, *The Digital Content Symposium*, 12 BERKELEY TECH. L.J. 1, 1 (1997) (emphasizing the importance of convening policymakers and lawyers in shaping digital content law).

2. The global Internet/Intranet market is estimated to grow tenfold by the year 2000, with corporate acceptance and adoption of new technology. John T. Mulqueen, *Money Savers: Surfing Down the Cost Curve*, COMMUNICATIONS WEEK, July 22, 1996, at 12.

3. Evan I. Schwartz, *Trust Me, I'm Your Software*, DISCOVER, May 1996, at 80 (discussing recent safety-critical software failures, including radiation therapy microprocessor software which overdosed and killed or seriously injured patients; missle timing software which could have been responsible for the deaths of twenty-eight soldiers in 1991; and a nuclear power plant's shut-down programs which were tested before the plant was open). Some hypothetical situations illustrative of potential personal injury:

> An energy management system in a high school that was programmed to be inoperable until 6:30 a.m. and that prevented an exhaust fan in a chemistry lab from working, thus causing a teacher to inhale chlorine gas . . . . A computer system that generated a warning label for a prescription drug that was inadequate and that the pharmacist failed to use anyway.

Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law Of Internet Security*, 10 HIGH TECH. L.J. 213, 258 (1995) (citing Thomas G. Wolpert, *Product Liability and Software Implicated in Personal Injury*, 60 DEF. COUNS. J. 519, 521 (1993)).

The first hypothetical has real life implications. *See, e.g.*, Bradley S. Davis, Note, *It's Virus Season Again, Has Your Computer Been Vaccinated? A Survey of Computer Crime Legislation as a Response to Malevolent Software*, 72 WASH. U. L.Q.

legal and cooperative regulation beyond the industry's current self-governance.[4]

Virus infections can potentially cause widespread, non-uniform damages similar to those personal injuries suffered in other mass torts; thus, in theory, the class action device might provide an attractive means to adjudicate these disputes and could serve to deter further outbreaks. However, litigating this type of Internet dispute presents unique challenges for determining the locus of the tort and personal jurisdiction. Further, classic tort and property analysis used to address copying, theft, or alteration of computer information within existing law has proved inconsistent and ineffective in resolving damages and liability issues. Courts' unsuccessful struggles to apply suitable property definitions to computer data and resources appear to erode the viability of a tort action, and courts tend to rely instead on contract law.[5] This reliance on contract law, rather than tort law, limits realistic redress for virus attacks to criminal actions.[6]

Courts and legislatures have not yet clarified standards of care or security guidelines for the software and networking community.[7]

411, 425 n.108 (1994) (describing the 1983 break-in by the "414 gang" into the Memorial Sloan-Kettering Cancer Center computer system in New York, where they gained access to radiation treatment data on over six thousand patients).

4. Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 10 (1994); Ilene K. Gotts & Alan D. Rutenberg, *Navigating the Global Information Superhighway: A Bumpy Road Lies Ahead*, 8 HARV. J.L. & TECH. 275, 278 (1995).

5. *See, e.g.*, Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis, 588 N.Y.S.2d 960, 963 (N.Y. Civ. Ct. 1992) (finding that if a computer consultant had breached the contract, then punitive damages were warranted by consultant's intentional misconduct).

6. *But see* Burleson v. State, 802 S.W.2d 429, 433 (Tex. Ct. App.—Fort Worth 1991, pet. ref'd) (requiring the offender to pay almost twelve thousand dollars in retribution). Texas's criminal statute permits civil liability for criminal violation. TEX. CIV. PRAC. & REM. CODE ANN. § 143.001 (Vernon 1997). *See also* 18 U.S.C. § 1030(g) (Supp. 1996). However, because virus outbreaks often result in economic losses not covered, this example may be an exception, not the rule.

7. *See generally* Rustad & Eisenschmidt, *supra* note 3, at 2-3; Vicky H. Robbins, *Vendor Liability For Computer Viruses And Undisclosed Disabling Devices In Software*, Vol. 10 No. 7 COMPUTER LAW 20 (1993) (discussing both contractual liability and liability in tort between software vendors and customers with regard to viruses and undisclosed devices). The industry has struggled to achieve compatibility through consortia such as the World Wide Web and the Internet Engineering Task

Because individuals who release viruses may be judgment proof, software distributors and on-line service providers present more lucrative targets and must adapt their business strategies to offset this increased risk of liability.[8]

This Note describes the Internet environment and the current legal framework in place available to address the problem of computer viruses, provides critical tort analysis of key issues, and examines these issues within current mass tort jurisprudence.

II. Computer Viruses and the Current Internet Infrastructure

Imagine surfing the Internet, doing research, or buying airline tickets online. Your computer might be susceptible to virus attacks while you transfer data. While you research, you might download virus-laden data from a bulletin board posted by someone else, which you unwittingly share with others. Sophisticated code might even be able to infect your machine as a consequence of simply visiting www.airline.com.[9]

Force, but has suffered from infighting. John Markoff, *Waging Internet War,* AUSTIN-AMERICAN STATESMAN, July 22, 1996, *available in* 1996 WL 3437621. For example, after it appeared that Microsoft would join Intel, Netscape, and Sun Microsystems in developing specifications for a technical standard for Internet security and privacy, Microsoft announced its intention to work against the consortium and published its own Internet Security Framework it intended to use as part of Windows. *Id.*

8. Scholars have recommended, *inter alia,* liability insurance, contractual disclaimer, and various secure computing strategies. *See infra* notes 107-117 and accompanying text.

9. The Princeton University group reported through April 1997 the contemporary security risks for Java and browser software which might subject Internet users to unexpected intrusions. *Secure Internet Programming: History* (last modified Apr. 30, 1997) <http://www.cs.princeton.edu/sip/History.html>. These specific security risks appear to have been fixed with the next release of software. *Id.* However, they represent vividly the ease with which a cleverly-designed virus might travel through the Internet. Further, users are susceptible until they are informed, and can upgrade to a safer program.

A. Malevolent Software and Its Impact

Computer viruses and their brethren (hereinafter "viruses") are generally programs intended to inflict some type of harm. Modern malevolent software is programmed to avoid detection—to extract itself if detected, to hide itself by various decryption methods or attachment of code which evades anti-viral software, or to embed itself in system boot software.[10] However, all rogue programs are not *per se* malicious. For example, some computer worms are programmed to search for resources, to execute tasks requiring inordinate amounts of computer time, or to coordinate operations between networks.[11]

There are generally four types of malevolent software programs: viruses, worms, time and logic bombs, and trojan horses. Viruses replicate and are usually intended to alter, harm, or destroy data. They attack disk boot sectors, operating systems, data, and applications. Even if not intended to be destructive, viruses can cause harm by consuming both human and computer resources.[12] Some viruses are merely intended to facilitate unauthorized access as a means of "electronic voyeurism."[13] "Worms" generally harm by altering data as they move through systems that they can access and erase themselves to avoid discovery.[14] "Time and logic bombs" are set to temporarily injure systems, or to attack specific users, types of code, or execute when certain conditions are met. "Trojan horses"

---

10. *See generally* Davis, *supra* note 3, at 2-3.

11. *See generally* Robert J. Malone & Dr. Reuven R. Levary, *Computer Viruses: Legal Aspects*, 4 U. MIAMI BUS. L. J. 125 (1994), *available in* 4 UMIABLJ 125 at *5 (stating several benefits derived from computer worms); Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime,* 16 RUTGERS COMPUTER & TECH. L. J. 1, 46-47 (1990).

12. Malone & Levary, *supra* note 11, at *3.

13. Branscomb, *supra* note 11, at 25.

14. "[A] 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.'" United States v. Morris, 928 F.2d 504, 505 n.1 (2d Cir.), *cert denied*, 502 U.S. 817 (1991). "It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." *Id.* Morris's "worm" had a programming error which allowed it to replicate, thus actually characterizing it as a virus. *Id.* at 506.

masquerade as potentially useful software programs or data but encompass a malevolent code, usually a virus, which infects and spreads when downloaded onto a new, unsuspecting host machine.

Potential damages are far reaching[15] and can result in enormous economic losses. An infamous worm set loose by Robert Morris in 1988 caused damages difficult to estimate, but which range from 6200 affected computers and $96 million in associated labor costs to higher estimates of $186 million to $1.1 billion.[16] Generally, a virus attack causes no hardware damage, and computer losses are confined to the information therein. Direct costs include restoration efforts to detect and eradicate the virus and to restore system operability and its lost data. Indirect costs include the loss of access to and use of information on both internal and external networks during those hours that computer systems are not operational.[17] However, as a result of virus attacks, disk crashes, and power outages which interrupt computer operations, most systems are now usually backed up and most of this information can be restored.

Entry points for viruses include distributed disks or software which originate in a machine affected by a virus, any networked system, and downloaded files across networks.[18] Widespread proliferation of a virus originally undetectable becomes compounded very quickly. Independent actors along the transmission chain can be unaware of malevolent software residing in their computer, network, files, or disks, even if they use virus protection software, because the software may not sufficiently detect more sophisticated code.[19]

---

15. *See* Davis, *supra* note 3, at 417 n.32 (noting that the 4096 virus originated in Israel and approximately three months later had infected sites across several U.S. states, including a Houston-based bank, Internal Revenue Service offices in Washington, California Burger King franchises, and Washington University in St. Louis).

16. Branscomb, *supra* note 11, at 8.

17. Some work may not be salvageable. For example, the Brain virus, which originated in Pakistan in 1986, caused one financial reporter six months of lost work, in addition to infecting three hundred computers at her newspaper office in Rhode Island. Malone & Levary, *supra* note 11, at *8.

18. Davis, *supra* note 3, at 427.

19. Examples include recent viruses affecting Java and Microsoft Word (and likely Excel, or any application program which uses macros). *See Deadly Black Widow on the Web: Her Name is JAVA* (May 5, 1996) <http://www.westol.com/~informer/guide/java.html>; *U.S. Department of Energy, CIAC*

These difficulties in detectability permit latency; thus, harm is broadly dispersed—both in time and form. Those programs deploying logic bombs lie dormant, awaiting a specific stimulus until they strike. For example, the Scores virus can selectively target specific companies.[20] Viruses can grow by replication until they clog memory or disk space, thus affecting systems differently according to their own configurations. Further, because some systems are more intelligently designed and can proactively detect invasive activity, "eggshell skull" victims with less sophisticated configurations may arguably suffer more damage from the same virus invasion.

B. The Internet Environment

The Internet is comprised of several independent but interconnected networks, originally implemented to facilitate scientific sharing of information.[21] The Internet has seen an extraordinary increase in use since President Clinton embraced the establishment of the National Information Infrastructure ("NII"), which now serves as the backbone of the Internet.[22] In 1996, the Internet linked over nine million host computers with an estimated forty million users, and carried over thirty million e-mail messages every day.[23] Among others, the banking industry has ventured online by adopting new Internet business strategies, utilizing "secure" environments developed by credit card companies.[24]

Information Bulletin, I-023: Macro Virus Update (January 28, 1998) <http://ciac.llnl.gov/ciac/bulletins/i-023.shtml>.

20. Malone & Levary, *supra* note 11, at *17.

21. The Advanced Research Projects Agency was the primary backbone of the Internet until 1990, but other governmental, educational, and commercial networks have been formed and interconnected over time. Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L. J. SCI. & TECH. 339, 381 n.20 (1996).

22. ACLU v. Reno, 1996 WL 933807, at *2 (E.D. Pa. Mar. 20, 1996).

23. Harold Smith Reeves, Comment, *Property in Cyberspace*, 63 U. CHI. L. REV. 761, 764 (1996).

24. Rustad & Eisenschmidt, *supra* note 3, at 237-38 (noting that joint ventures between American Express and America Online, and Visa International and Microsoft, for example, will enable private and secure communications across the Internet).

Most computers access the Internet by establishing a telephone connection to an Internet online service provider ("ISP") computer, which provides news, mail and bulletin board services, and routes data from the computer to the rest of the Internet. Larger organizations, including ISP's, connect to networks of computers on the Internet through high-speed telephone lines. Most businesses also link intracompany computers together to facilitate electronic transfer and sharing of programs, data, e-mail, and printers.[25] Larger companies and educational institutions generally install routers or gateways for their distributed computing networks to manage traffic, filter messages to external recipients, and allow direct access to the Internet.[26] These office networks become a part of the Internet network. These configurations introduce the potential for widespread, virtually instantaneous distribution and corruption at each way station.[27] Data travels over the Internet subject to little or no control through a series of intermediate computer servers, and can "pollute" millions of paths virtually at the speed of light.

A computer that is networked into the Internet is susceptible to break-ins by hackers who can breach the security of its firewall, if it has one.[28] Each Internet user may be infected with a virus from downloading software or shareware that they request, or through a bulletin board.[29] An even larger threat for large numbers of Internet

---

25. *Id.* at 220 (explaining that many companies provide their own internal version of the Internet on an Intranet).

26. *Id.*

27. The Morris worm is illustrative: it reached about ten percent of the sixty thousand computers on the Internet within three hours of its release. Reeves, *supra* note 23, at 765 n.17.

28. Branscomb, *supra* note 11, at 2; Rustad & Eisenschmidt, *supra* note 3, at 227-28. But a firewall provides no protection when an "attack is launched from behind" it, as might be the case with malicious Java applets, which can foil Web browser software resident on users' computers. *Java Black Widows— Sun Declares War* (visited Jan. 30, 1998) <http://www.infoave.net/sbn/obc.html>.

29. Most virus issues arise in on-line systems or on-line access as compared to distributed software products on diskette. *U.C.C. 2B (Draft)* (last official draft Sept. 25, 1997) <http://www.law.uh.edu/ucc2b/092597/092597_2b.html>. The ALI and National Conference of Commissioners on Uniform State Laws are revising a draft of Article 2B to the UCC. Dowloaded software and online transactions are expressly excluded from the new UCC, which otherwise permits mutual contractual disclaimers for viruses. § 2B-313(c), Reporter's Note. *But see* Susan C. Lyman, *Civil Remedies for the Victims of Computer Virus*, 11 COMPUTER L.J. 607, 631 (1992) (finding that the

users is likely the kind of rogue software which could breach security measures in Internet and browser software such as Netscape Navigator.[30] These infections might allow a virus to access users' DOS machines after accessing a Web page; to modify data between a victim's machine and all other Web servers on the Internet; and to masquerade as "trusted" software, which would allow it to completely circumvent the browser's security.[31] No direct access by a rogue programmer is required to infect remote users broadly dispersed over various jurisdictions.[32] In fact, anyone who can access a company server with the appropriate application software can access the Internet through a cellular phone keypad.[33] Companies and governmental offices are more likely hacker targets, and thus must be able to ward off the break-ins which have deterred some firms from connecting to the Internet.[34]

III. Statutory Framework

Tort law over the Internet must be developed within the rubric of the patchwork of federal and state regulations governing the NII.[35]

---

larger threat is through software programs, rather than bulletin boards, because users accept the risk of viruses in exchange for free access). This acceptance of risk is arguable. *See infra* note 208 and accompanying text.

30. *Deadly Black Widow on the Web: Her Name is JAVA* (May 5, 1996) <http://www.westol.com/~informer/guide/java.html>.

31. *Secure Internet Programming: History* (last modified Apr. 30, 1997) <http://www.cs.princeton.edu/sip/History.html>. Even though these problems appear to be fixed in subsequent releases after security flaws in the software are reported, they still provide a window of opportunity for viruses to cause widespread damage.

32. The *Morris* court held that Morris's use of the sendmail and finger programs constituted unauthorized access, allowing the court to convict Morris within the contours of the statute. United States v. Morris, 928 F.2d 504, 510 (2nd Cir. 1991).

33. Mulqueen, *supra* note 2, at 35.

34. *See* Rustad & Eisenschmidt, *supra* note 3, at 218-20. While the increases in break-ins by more than seventy percent in 1994 and 1995 does not match the growth of the Net itself, viruses are still an invidious problem.

35. Regulations are divided into federal communications, cable, and wireless media; electronics and computer privacy, computer security, and intellectual property laws; and consumer credit, financial, and medical information. Gotts & Rutenberg, *supra* note 4, at 279.

While judicial recognition of property interests under tort law for data damaged due to viruses has been virtually nonexistent, it appears that this trend may be changing.[36] Legislatures have begun to explicitly protect computer data from tampering, destruction, alteration or access under their criminal computer statutes, and to permit civil redress therein for harms incurred, which statutorily protects legal interests in the computer data damaged.

A. Federal Statutes[37]

1. Computer Fraud and Abuse Act (the "CFAA")[38].—Revisions to the original CFAA have furnished the law with much-needed teeth in the war against the growing problem of computer saboteurs operating "computers in interstate commerce or communication."[39] The Act now protects against the impairment, or potential impairment to the integrity or availability of data, computer systems, information, or programs upon unauthorized access.[40] The amended legislation provides for civil liability for intentional actions where the receipt of the harmful code is unauthorized, but the aggregate damage must be at least five thousand dollars.[41] The CFAA now criminalizes conduct committed "in furtherance of any . . . tortious act in violation of the . . . laws of the United States or of any State."[42]

---

36. *See generally* Rustad & Eisenschmidt, *supra* note 3, at 254.

37. For a more detailed analysis of such criminal statutes, see Alois Valerian Gross, *Criminal Liability For Theft Of, Interference With, Or Unauthorized Use Of, Computer Programs, Files, Or Systems*, 51 A.L.R. 4th 971 (1995).

38. 18 U.S.C. § 1030 (Supp. 1996).

39. 18 U.S.C. § 1030(e)(2) intentionally broadened coverage of the Act to include computers connected to the Internet. For example, the Senate Committee on the Judiciary intended that the medical care clause of 18 U.S.C. § 1030(a)(5) (1994) covers situations in which data alteration was possible, such as in the Sloan-Kettering break-in. *See* Davis, *supra* note 3, at 425 n.108.

40. 18 U.S.C. §§ 1030(a)(5), (e)(8). Subsection (A) proscribes intentionally caused damage; (B) covers recklessly caused damages; and (C) covers damages caused by intentional access. *Id.* § 1030(a)(5)(A)-(C).

41. *Id.* § 1030(g) (providing that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator . . . .").

42. *Id.* § 1030(c)(2)(B)(ii).

2. *Electronic Communications Privacy Act*[43].—This statute proscribes access to, or alteration of, transactional records or stored wire and electronic communications where a perpetrator is unauthorized to access the computer or its records. Violation of this statute creates civil liability for providers of electronic communications services, subscribers, or customers resulting from this knowing or intentional access.[44] The court in *American Computer Trust Leasing v. Jack Farrell Implement Co.*[45] granted defendant software licensor summary judgment under 18 U.S.C. § 2707 after it deactivated its licensee's software for nonpayment, because the statute bars only unauthorized access, and the parties' license agreement granted access.[46] Because most victims of an intentional virus attack do not generally authorize access to their computers,[47] they may be able to maintain an action under this statute.

3. *Economic Espionage Act*[48].—This criminal statute proscribes not only the misappropriation of trade secrets, but any alteration, destruction, replication, or transmission over a network thereof.[49] It not only broadens criminal liability for behavior regarding trade

---

43. 18 U.S.C. § 2701 (1994).

44. *Id.* § 2707.

45. 763 F. Supp. 1473, 1480 (D. Minn. 1991), *aff'd, remanded sub nom.* American Computer v. Boerboom Int'l, 967 F.2d 1208 (8th Cir. 1992), *cert. denied*, 506 U.S. 956 (1992).

46. The court also granted summary judgment on claims for conversion and nuisance because Minnesota law did not legally protect computer data as property. *Farrell*, 763 F. Supp. at 1493-94. Neither MINN. STAT. ANN. § 332.51 nor § 645.21 could be applied retroactively for computer theft or damage. *Id.* at 1493.

47. The success of this argument is subject to the validity of web wrap licenses, discussed *infra* notes 153 and 206-7 and accompanying text.

48. 18 U.S.C. § 1831 (1996).

49. 18 U.S.C. § 1831(a) addresses a perpetrator who:

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice or deception obtains a trade secret;
>
> (2) without authorization copies, duplicates, . . . downloads, uploads, alters, destroys, . . . replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization . . . .

secrets, but also includes intangible and electronically stored trade secrets.[50] The recent investigation into whether Reuters would be liable for allegedly 'stealing' Bloomberg's confidential operating systems software provides an excellent example of the kind of behavior the Act intended to prevent.[51] Reuters allegedly devised a scheme for electronically breaking into Bloomberg's computers in order to use it to Bloomberg's competitive disadvantage.[52] However, it is unlikely that the average hacker who releases a virus would be liable under this statute for damage to trade secrets because the statute likely requires a financial motive.[53]

4. Wire fraud[54].—This federal legislation prohibits confidential schemes to obtain information by false representations or pretenses in its abstract, intangible form.[55] In *United States v Seidlitz*,[56] a former employee was found guilty of intent to defraud for accessing the company mainframe through interstate wire and retrieving a confidential computer program. The court reasoned that the appropriated data was a valuable company trade secret because the company enjoyed a competitive advantage due to its expensive modification of the system and the corresponding measures it employed to prevent unauthorized access.[57] However, the court declined to convict Seidlitz for interstate

---

50. James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 188-92 (1997).

51. Kurt Eichenwald, *Reuters Unit is Investigated Over Theft of a Rival's Data*, N.Y. TIMES, Jan. 30, 1998, at A1, C18.

52. *Id.* at C18, c1-2.

53. Pooley, Lemley & Toren, *supra* note 50, at 194 (discussing that § 1832 requires "intent to convert a trade secret," which arguably incorporates the criminal law of conversion).

54. 18 U.S.C. § 1343 (1984). Information is protectible under § 1343 if it has economic value. Eli Lederman, *Criminal Liability For Breach Of Confidential Commercial Information,* 38 EMORY L.J. 921, 987 (1989).

55. 18 U.S.C. § 1343 provides for fine or imprisonment for devising:

> any scheme or artifice . . . for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . .

56. 589 F.2d 152, 153 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979).

57. *Id.*

transportation of stolen property.[58] It is conceivable that a hacker who devises a scheme to capture credit card numbers with a virus and then destroy his victim's records, which likely have some "black market" value, would be culpable under this Act. However, because most virus infections appear to be targeted to cause damage, rather than to obtain property, this statute may not serve as a deterrent.

5. National Stolen Property Act[59].—This Act proscribes the transportation in interstate commerce of stolen or converted property.[60] Courts have generally held that the common and usual meaning of the language encompasses tangible rights, not those incorporeal or intangible.[61] In *United States v. LaMacchia*,[62] LaMacchia provided software to be posted on a bulletin board for downloading without charge.[63] In dismissing the complaint, the court relied on *Dowling v. United States*,[64] which reasoned that copyright infringement could not be used as a basis for a conviction under section 2314, because the statute required a corporeal taking.[65] It is arguable that this statute should not reach Internet theft across state lines.[66] Thus, a virus programmed to "steal" credit card numbers or

---

58. *Id.* 18 U.S.C. § 2314 (1997) did not apply to Seidlitz because intangible electromagnetic signals did not constitute goods or wares. *Id.* at 154 n.3.

59. 18 U.S.C. § 2314.

60. 18 U.S.C. § 2314; 18 U.S.C. 2315 (1997).

61. Lederman, *supra* note 54, at 978. *See* United States v. Dowling, 473 U.S. 207, 228-29 (1985) (holding that criminal penalties did not reach the interstate transportation of "bootleg records" because the items were not "stolen, converted or taken by fraud" except by being manufactured and distributed without the consent of the copyright owners); United States v. Brown, 925 F.2d 1301, 1306-7 (10th Cir. 1991) (dismissing the indictment on the grounds that computer programs, software, and source code were not the type of property contemplated within "goods, wares, or merchandise" as specified in the statute). *But see* United States v. Riggs, 739 F.Supp. 414, 420 (N.D. Ill. 1990) (recognizing a downloaded file as a "good, ware, or merchandise" within the purview of the statute, and declining to require tangibility).

62. 871 F. Supp. 535 (D. Mass 1994).

63. *Id.* at 536.

64. 473 U.S. 207 (1985).

65. *Id.* at 217. The No Electronic Theft ("NET") Act expressly overruled the *LaMacchia* decision in order to protect potential infringement of copyright interests by electronic means. No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (Dec. 16, 1997).

66. Pooley, Lemley & Toren, *supra* note 50, at 183 (discussing that permitting cases involving intangible property would likely lead to undesirable results).

passwords across the Internet would probably not trigger a violation under this statute because the Act does not involve tangible property.

B. State Criminal Statutes

Most states have enacted criminal legislation that is more expansive than the CFAA in an effort to improve their arsenals in the fight against computer sabotage.[67] For example, Minnesota defines destructive computer programs as those which degrade performance, produce unauthorized data, destroy or perform unauthorized alterations of data, or produce other destructive computer programs.[68]

Information within a computer or stored on a disk is now included as "property" in some states that follow Massachusetts's approach. Massachusetts prosecutes offenders under existing legislation proscribing theft and conversion,[69] which effectively covers acts which "alter, damage, delete or destroy" computer programs or files. Alabama and Wyoming adopted another approach by addressing the issue of computer abuse within the purview of intellectual property.[70]

New York expanded its definition of property to include computer data or programs by prohibiting acts of malevolent transmissions or "computer tampering."[71] A New York court found a defendant guilty of both computer tampering and breach of contract

---

67. Davis, *supra* note 3, at 428. *See, e.g.*, Lyman, *supra* note 29, at 613-623 (providing a more in-depth discussion of several state statutes which specifically provide civil remedies for computer crimes).

68. MINN. STAT. ANN. § 609.87(12) (West Supp. 1993); Davis, *supra* note 3, at 429.

69. MASS. GEN. LAWS ANN. ch. 266, § 30(2) (West Supp. 1988) (noting that the statute encompasses "electronically processed or stored data, either tangible or intangible," as well as "data while in transit . . . ."). Montana includes in its definition of property, "electronic impulses, electronically processed or produced data or information, . . . computer software or computer programs," as well as computer services. MONT. CODE ANN. § 45-2-101(59)(k) (1995).

70. *See, e.g.*, ALA. CODE § 13A-8-102 (Supp. 1992) (classifying electronic data as intellectual property).

71. N.Y. PENAL LAW §§ 156.20, 156.25-.27 (Consol. 1984 & Supp. 1994) (prohibiting an actor from accessing a computer or computer service to intentionally alter in any manner or destroy computer data or a computer program of another person).

after he installed a logic bomb which crashed the plaintiff's computer system, allegedly to ensure that he was paid.[72] The plaintiff was unable to use its system for claims or billing purposes, and was awarded under a breach of contract claim both compensatory as well as punitive damages for a total of twenty-five thousand dollars.[73] A Texas court convicted a defendant for harmful access to a computer after he destroyed company payroll data by inserting a malicious code into a company computer.[74]

Software vendors' ability to resort to self-help electronic repossession originally fell under siege in 1994 and 1995, when the Virginia legislature unsuccessfully attempted to enact a criminal statute to require vendors to provide written notice of disablement code.[75] A few courts have begun to define the limitations for self-help restraints, and permit them where parties to software contracts expressly allocate risks between themselves.[76]

IV. The Challenge in Tort

Actions in tort present new problems for the courts because they have not considered computer information to be legally protected property; thus, losses are generally economic.[77] The global nature of the Internet also presents a unique challenge in the analysis of liability

---

72. Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis, 588 N.Y.S.2d 960, 961 (N.Y.Civ. Ct. 1992).

73. *Id.* at 963. The New York legislature responded to this case by making computer tampering a felony in order to further deter malicious attacks. N.Y. PENAL LAW §§ 156.25-.27 (Consol. 1984 & Supp. 1994).

74. Burleson v. State, 802 S.W.2d 429, 432 (Tex. App.—Fort Worth 1991, *writ ref'd*). The court sentenced him to seven years probation, and ordered him to pay $11,800 in restitution. *Id.*

75. Ester C. Roditti, *Is Self-Help A Lawful Contractual Remedy?*, 21 RUTGERS COMPUTER & TECH. L.J. 431, 448-49 (1995). The bill was prompted by a 1993 incident in which a large shipbuilding company was allegedly nearly paralyzed due to a deactivation device placed in its software by a software vendor, as a result of a dispute over terms of the software license. *Id.* at n.118.

76. *See infra* notes 134-41 and accompanying text.

77. Recent court decisions and criminal legislation passed indicate a shift towards recognition of damage for the loss of computer use. *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 1997 WL 109303 (S.D. Ohio Feb. 3, 1997); Thrifty Tel, Inc. v. Bezeneck, 46 Cal. App. 4th 1559 (1996).

for widespread, remote harms resulting from a single virus attack, or leave issues such as personal jurisdiction and causation, to which the determinative inquiry is foreseeability.[78]

Implementing standards of care to regulate behavior spreads the risk of doing business electronically to all users, rather than imposing that burden on those hit with virus attacks. Imposing appropriate tort liability for viral infection should improve market efficiency and confidence in the system by managing realistic business expectations. Parties such as software providers can limit to some extent their risk of liability by contract by disclaimer or limitations on liability and notice of disabling restraints.[79] Individuals and businesses will then participate to the degree of risk feasible to them.[80]

A. Potential Parties to Actions in Tort

Foreseeable victims suffering damages to legally protected property can maintain a civil tort action or bring suit under those criminal statutes that permit such civil remedy. However, in jurisdictions where computer data is not considered property, most virus damages will be considered unrecoverable economic losses.

Products liability requires no privity with a seller of the defective product.[81] Thus, anticipated and reasonably foreseeable purchasers, consumers, and users might ostensibly maintain suit for damages from software defectively infected by a virus. Foreseeable bystanders such

---

78. For example, if the data's path is foreseeable, then an Internet user who intentionally transmits data may be properly subject to personal jurisdiction for resulting harms to those foreseeable plaintiffs. Calder v. Jones, 465 U.S. 783, 789-90 (1984). Jurisdictional issues regarding the Internet are complex and outside the scope of this article. *See generally* Zembek, *supra* note 21, at 379; Harry H. Perritt Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. R. 1 (1996); Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J.L. & TECH. 3 (1997).

79. Robbins, *supra* note 7, at 22-24. The extent to which these disclaimers will be enforceable is questionable. *See infra* note 206 and accompanying text.

80. Insurance, regulatory standards, contract law, and criminal law will probably govern cyberspace to some extent. *See generally* Branscomb, *supra* note 11, at 57-58; Rustad & Eisenschmidt, *supra* note 3, at 263-64.

81. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 100, at 704 (5th. ed. 1984).

as parties accessing an infected company's computer could also potentially sue for products liability.

In most cases, target defendants will ultimately be employers of the tortfeasors who distribute the virus, such as software companies, ISPs, bulletin board systems ("BBS") operators, or data repositories, as individuals responsible for releasing a virus are likely to be judgment proof. Corporations and service or software providers will be held liable for their employees' negligent acts where the acts are within the scope of employment, even if the employer has not authorized them.[82]

The definition of "seller" within the *Restatement (Second) of Torts*, section 402A has grown to encompass those defendants for whom the policies behind the theory would be applicable.[83] It appears that anyone in the distribution chain of a software product—such as vendors, licensors, or installers—might be liable to potential plaintiffs, with an opportunity for contribution from the party or parties ultimately responsible for the defect.[84] Thus, liability might lie for software providers who knowingly distribute or sell software over the Internet when a defect permits a virus infection.[85] A maker of anti-

---

82. *Id.* § 70, at 506.

83. Courts have been convinced that strict liability should lie where: (1) costs can be borne by the enterprisers who make and sell products which cause damage; and (2) elimination of the necessity for proving negligence will promote the cause of accident prevention, reduce litigation costs, and generally provide effective accident deterrence. *Id.* § 98, at 693.

84. *Id.* § 100, at 704-06. *See, e.g.*, Sparacino v. Andover Controls Corp., 592 N.E.2d 431, 434-35 (Ill. 1992) (finding vendor not liable for a software system that was not dangerous as assembled, but suggesting that because installation of the software created a dangerous condition, installer may have had a duty to warn). *But see* Lyman, *supra* note 29, at 632 (concluding that, although the policy motivations for applying strict products liability apply to the software industry, virus-infected software is not considered unreasonably dangerous); Patrick T. Miyaki, Comment, *Computer Software Defects: Should Computer Software Manufacturers be Held Strictly Liable for Computer Software Defects?*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 121, 143-44 (holding software manufacturers strictly liable for defects would chill growth of innovative software products).

85. For example, even after Netscape provided software updates and announcements to contain the security flaws found in its software, software lacking the new security updates remained on the market. *Java Black Widows—Sun Declares War* (visited Jan. 30, 1998) <http://www.infoave.net/sbn/obc.html>.

virus software might also be subject to products liability for failing to detect viruses or failing to warn users of its software's limitations.[86]

B. *Industry Standards*

The Internet computer industry is still developing standards for conduct, thus providing the courts little guidance. Software providers, ISPs, and other members of the World Wide Web Consortium and Internet Engineering Task Force have not agreed to standards for network security.[87] Furthermore, neither software programmers nor consultants are licensed, and most courts do not consider them liable for malpractice.[88]

The market has historically self-regulated virus crises resulting from software distribution, usually by the software providers' recall or upgrade of the product or distribution of anti-viral software.[89] This occurred after Novell, Konami, Intel Corporation, Da Vinci Systems,

---

86. For example, the software might fit within the contours of § 402A of the *Restatement (Second) of Torts* where it was a subcontracted portion of mission-critical software for a nuclear plant. One author notes that complex, mission-critical software is "too complex to test," and that "guaranteed system behavior is impossible to achieve." Schwartz, *supra* note 3, at 80.

87. Markoff, *supra* note 7. In 1996, after Netscape's response to security flaws in its software did not effectively remove the at-risk software from the market, Stephen Cobb, Director of Special Projects for the National Computer Security Association, opined that "[t]he situation is scary. Software companies are releasing products on the Internet without even considering the hacker perspective." *Deadly Black Widow on the Web: Her Name is JAVA* (May 5, 1996) <http://www.westol.com/~informer/guide/java.html>.

88. *See* Hospital Computer Sys. v. Staten Island Hosp., 788 F. Supp. 1351, 1361 (D. N.J. 1992) (stating that computer consultants do not meet the standard of "professionals" and thus can be held liable only for ordinary, not professional, negligence); Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 479 F. Supp. 738, 741 n.1 (D. N.J. 1979) (rejecting new tort of "computer malpractice" for those who render computer sales and service), *aff'd*, 635 F.2d 1081 (3d Cir. 1980). *But see* Diversified Graphics v. Groves, 868 F.2d 293, 297 (8th Cir 1989) (holding computer consultants to elevated standard of care because of their superior knowledge and expertise in computer systems).

89. Robbins, *supra* note 7, at 20-21. A few cases have reached the courts. *See, e.g.*, Coastal Credit Co. v. CSS, Inc., 685 So. 2d 464, 465 (La. 1996) (dismissing, for lack of personal jurisdiction, plaintiff's claim for damages from purchased software which had been infected with Michelangelo virus). Courts have also addressed some issues regarding self-help devices. *See infra* notes 132-142.

and Access Software released software products suffering from various viral infections to customers and distributors, and leading Edge Products shipped computers to resellers with hard disks infected by the Michelangelo virus.[90] Microsoft distributed free anti-viral software in an attempt to eradicate the Microsoft Word macro virus,[91] which infected numerous users through templates passed as trojan horse documents. Recent security flaws in Java software exposing Internet users to virus attacks have been resolved in later upgrades after being reported to the online community.[92] However, viruses can attack during this delay between the product release and subsequent upgrade, and even beyond this period, where older versions of software are sold or used.[93]

However, market expectations might be better managed by using the risk-utility test, under which the operative inquiry is the balance between the utility of the relevant conduct and the likelihood and extent of harm imposed on foreseeable plaintiffs.[94] The market now provides enough statistics indicating both high risk and potentially widespread damage from virus attacks, while either programming prevention or off-the-shelf capabilities to detect viruses may impose a proportionally smaller burden.[95] Although viruses have caused

---

90. Robbins, *supra* note 7, at 26-27.

91. *U.S. Department of Energy, CIAC Information Bulletin, I-023: Macro Virus Update* (January 28, 1998) <http://ciac.llnl.gov/ciac/bulletins/i-023.shtml>.

92. *Secure Internet Programming: History* (last modified Apr. 30, 1997) <http://www.cs.princeton.edu/sip/History.html>.

93. *Java Black Widow—Sun Declares War* (visited Jan. 30, 1998) <http://www.infoave.net/sbn/obc.html>.

94. KEETON, *supra* note 81, § 32, at 170-72.

95. It is likely impossible to eradicate viruses completely, thus precluding the possiblity of a bright-line market standard. Simply disinfecting a computer system could cost a staggering amount. In 1990, computer infection in the United States alone was estimated to be one percent, or about 500,000 computers. Joseph Daly elaborates:

> Further, assuming that it would take a mere 20 hours to disinfect a system, at a conservative estimate of a $15 per hour service charge, the national bill for only a one percent infection rate would be $150 million. A survey conducted in 1989 however, found that 10 percent of the respondents had personally suffered a computer virus, and that 23 percent knew of someone who had been infected. This suggests a far greater amount of monetary damages. In the private sector, one corporation in Texas was infected, requiring its 3,000 computer network to shut down for four days. It took 50 computer analysts to remove the virus, even though the team discovered

millions of dollars in documented economic loss to victims, these losses have not been recoverable in tort. Because no personal injuries have been suffered thus far, there is probably no driving impetus to establish liability, as there was after the industrial revolution.[96] As a result, the entire industry may need more guidance in expediting a "prudent care" standard referred to in *The T.J. Hooper*.[97] Using this approach, the standard of care would be that which a prudent provider or software programmer would do under the circumstances.[98]

Courts are now formulating standards for service providers in defamation and copyright litigation, in the wake of Clinton's Working Group on Intellectual Property and the NII.[99] One recent case, *Religious Technology Center v. Netcom*[100] held that liability for

---

> that only 35 computers were actually infected. The total costs to the corporation however, including lost revenues, was $10 million. Unfortunately, even having a virus removed provides no guarantee of safety from further virus harm. In the United States, 90 percent of all infected users experience re-infection within 30 days of having the original virus removed.

Joseph Daly, *The Computer Fraud and Abuse Act—A New Perspective: Let the Punishment Fit the Damage*, 12 J. MARSHALL J. COMPUTER & INFO. L. 445, 464, 465 (1993) (citing David Stang, *PC Viruses: The Desktop Epidemic*, WASH. POST, Jan. 14, 1990, *available in* 1990 WL 2154620).

96. Rustad & Eisenschmidt, *supra* note 3, at 260.

97. 60 F.2d 737, 740 (2d Cir. 1932), *cert. denied*, 287 U.S. 662 (1932). Learned Hand reasoned:

> [I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests . . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.

Id. at 739.

98. *See* Nimmer, *infra* note 146, § 10.13[2], at 10-37.

99. The White Paper recommends subjecting service providers to strict liability for copyright infringement for uploading infringing materials because lowering the standard would result in a "significant departure from current copyright principles and law and . . . a substantial derogation of the rights of copyright owners." Rustad & Eisenschmidt, *supra* note 3, at 254.

100. 907 F. Supp. 1361, 1375 (N.D. Cal. 1995) (denying Religious Technology Center's (RTC) claim for vicarious liability and granting Netcom's motion for summary judgment for direct infringement, after Netcom refused to deny subscriber access to its system after the subscriber posted RTC copyrighted works on Netcom's BBS).

causing distribution of copyrighted works should rest with the subscriber posting them, and not with the BBS provider, whose actions were automatic and indiscriminate; otherwise, an infringment theory would be unworkable because it would "hold the entire Internet liable for activities that cannot reasonably be deterred."[101] Though it raised a question of fact regarding vicarious liability as to Netcom's right and ability to control its subscriber's conduct, RTC failed to raise an issue of fact regarding any direct financial benefit gained from its user's activities.[102] The court in *Stratton Oakmont, Inc. v. Prodigy Services*[103] held Prodigy liable for defamatory statements posted on its bulletin because it had exercised some editorial control. The 1996 Telecommunications Act expressly overruled *Stratton* in light of the importance of promoting growth on the Internet.[104]

---

101. *Id.* at 1372. *See also* Cubby v. Compuserve, 776 F. Supp. 135, 140 (S.D.N.Y 1991) (rejecting Compuserve's liability for posting defamatory statements because it should be entitled to higher protection as a news publisher, which requires knowledge). *But cf.* Playboy, Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (holding the BBS operator liable for violating the plaintiff's right to publicly distribute and display copies of digitized pictures from its copyrighted magazine by posting the pictures without permission); Sega, Ltd. v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996) (finding that BBS's knowledge of infringing activities, solicitation of uploading copies of Sega's video games, and direction and provision of its facilities constituted contributory infringement).

102. *Netcom*, 907 F. Supp. at 1372.

103. No. 31063/94, 1995 N.Y. Misc. LEXIS 229 at *5-6 (Nassau County N.Y. Sup. Ct. May 26, 1995) (distinguishing *Cubby v. Compuserve* because Prodigy regulated postings on its bulletin boards by (a) promulgating content guidelines, (b) using software that automatically prescreened all bulletin board postings for offensive language, and (c) using "Board Leaders" to enforce Prodigy's content guidelines).

104. 47 U.S.C. § 230(b)(1)-(5) (1997) states:

> It is the policy of the United States:
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online

No courts have addressed the issue of liability for service providers for defective software or virus infections, but it stands to reason that they would consider this same policy. While the White Paper calls for strict liability to protect owners' copyright interests, strict liability appears too harsh a standard to impose in a largely commercial setting.

Subjecting ISPs, vendors, licensors, or installers to the same standard of care as manufacturers for transmissions of viruses in a product distribution line might provide a more workable approach.[105] Requiring implementation of security devices such as firewalls, audit controls to track potential intentional tortfeasors, or other virus detection mechanisms would ensure a reasonable means to avoid receiving and transmitting viruses.[106] Although adequate security mechanisms appear to be necessary, this requirement needs to be balanced with the potential liability an ISP or may face for unwittingly permitting transmissions of rogue code.[107]

Adequate security levels will vary from off-the-shelf virus scanning software to security plans administered by consultants or in-house personnel, who will assess the fragility of the computer systems and networks and recommend products, services, or system maintenance plans. Licensing security specialists as NII development progresses may improve the quality and consistency of security standards, but it may also subject the specialists to malpractice.[108]

Moreover, because phone, TV, and satellite communications media are heavily regulated as part of the stream of interstate

---

material;

(5) to ensure the enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

105. Rustad & Eisenschmidt, *supra* note 3, at 254.

106. David L. Gripman, Comment, *The Doors Are Locked But The Thieves And Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 192-94 (1997) (suggesting that corporations be held liable for online torts if they do not meet minimum security standards); Lyman, *supra* note 29, at 634 (suggesting that adequate security measures accompanied by insurance coverage may provide effective alternatives to civil or criminal actions).

107. New viruses which may be temporarily undetectable present the problem for holding ISP's or software providers strictly liable.

108. Rustad & Eisenschmidt, *supra* note 3, at 250.

commerce,[109] similar government agency standards might be adopted to address virus detection, eradication, and prevention.[110] The Cyber Security Assurance Group was formed to aggressively address the issue of computer tampering.[111] U.S. and international regulation of a global Internet must balance the tension between protection of data in the stream of commerce and rights to privacy, so as not to further disenchant the international community.[112]

One author has suggested that deterrence of unauthorized access be managed through a contract law paradigm.[113] Access to participating sites and providers would be limited to users who sign agreements to abide by a model code. Another scholar rejects this paradigm because the code's uniformity presents unfair bargaining issues similar to shrinkwrap licenses.[114] He suggests that limiting access through adhesion contracts would divide—and thus destroy—the Internet, and suggests non-uniform, bargained-for contracts for use in conducting online commerce.[115] Another author suggests that providers carry liability insurance.[116]

---

109. Thus, tension must be balanced between commerce and First Amendment issues. *See* Gotts & Rutenberg, *supra* note 4, at 337.

110. The National Computer Security Center administers C2 certification of computer security for computer systems used in government activities. Rustad & Eisenschmidt, *supra* note 3, at 251. Internet companies might be required to obtain necessary "trusted certificate" authority for validating digital signatures, or be found negligent *per se* for any loss resulting from such failure, a higher standard than exists today. *Id.* at 251-52 n.188.

111. The Justice Department recently doubled its computer crime unit and created an Information Warfare technology center, and formed new FBI computer crime squads. Bill Frezza, *Fear Mongering: 'Just say No to Cybercrats,'* COMMUNICATIONS WEEK, July 22, 1996, at 45.

112. *See, e.g.*, Kristi Essick, *Net Privacy is International Concern*, 10 SUN WORLD ONLINE (Aug. 8, 1996) <http://www.sun.com/sunworldonline/sw01-08-1996/swd-08-usenix.html>.

113. Dunne, *supra* note 4, at 12-13.

114. Mark A. Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311, 317-18 (1995).

115. *Id.* at 321, 323.

116. Branscomb, *supra* note 11, at 57.

C. *Liability*

Judicial recognition of civil liabilities in virus cases appears to be increasing, clarifying the interpretation of earlier cases which never reached a determination of the merits.[117] The court in *North Tel, Inc. v. Brandl*[118] affirmed a default judgment in bankruptcy court for actual damages suffered as a result of defendant's intentionally released computer virus, but did not rule on the plaintiff's claims for intentional interference with business relations and prospective business advantage, conversion, and nuisance.[119] In addressing intent, however, the court found that Minnesota law for conversion requires only a willful interference, and that nuisance is broadly actionable for "intentional conduct, negligence, . . . or some other tortious activity . . . ."[120] Another case where a disabling device locked up the plaintiff's computer system was settled under terms of nondisclosure.[121] Revlon sued Logisticon under tort theories of intentional interference with contractual relations and prospective economic advantage, misappropriation of trade secrets, and breach of contract and express warranty.[122]

Although substantive tort law varies widely from state to state, courts may find that those who intentionally release viruses should be liable for intentional torts, including trespass to chattels, conversion, interference with contract or business relations, and even nuisance. Non-intentional releases of viruses where, for example, a software provider would be vicariously liable for a negligent employee who fails to adequately screen for or adequately program safeguards

---

117. Since several state criminal statutes recognize computer data as a legally protected interest, courts may soon follow suit. *See supra* notes 68-74 and accompanying text.

118. 179 B.R. 620 (Bankr. Minn. 1995).

119. *Id.* at 627-28. The defendant intentionally "altered and damaged [plaintiff's] computer, computer systems, computer network and computer software," and "deprived Plaintiff of the use and possession of the contents of its computer system"; he also pled that defendant's placing a virus in the computer constituted a nuisance. *Id.* at 625.

120. *Id.* at 625.

121. Revlon, Inc. v. Logisticon, Inc., No. 705933 (Cal. Super. Ct. Santa Clara County, complaint filed October 22, 1990).

122. *Id.*; Robbins, *supra* note 7, at 22 n.35.

against viruses, might subject the provider to liability for negligent misrepresentation, negligence, or even strict products liability, especially if damage to computer information is held to be damage to property such that claims are not barred by the economic loss rule.

1. Intentional torts.—Liability may lie where a defendant intentionally and improperly interferes with the plaintiff's rights under a contract with another party, if the interference causes the plaintiff the loss of rights under the contract or makes the rights under the contract more costly or less valuable.[123] *Brandl* illustrates a fact pattern that appears to support an action for tortious interference with contractual relations. The defendant intentionally transmitted a virus to North Tel's computers, which were known to be used for business purposes, and the damage caused by the virus interfered with business operations.[124]

Conversion is "an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."[125] Trespass to chattels subjects the trespasser to liability for "harm thereby caused to such other's interest in the chattel," and includes any direct and immediate intentional interference to "damage goods or destroy them, to make an unpermitted use of them, or to move them . . . ."[126]

Two recent decisions may indicate a shift from the more traditional approach seen in computer litigation. In *American Computer Trust Leasing v. Jack Farrell Implement Co.*,[127] the court granted summary judgment for the defendant on plaintiff's trespass claim[128] and refused the nuisance claim.[129] However, in *CompuServe*

---

123. KEETON, *supra* note 81, § 129, at 978.

124. North Tel., Inc. v. Brandl, 179 B.R. 620, 622 (Bankr. Minn. 1995).

125. RESTATEMENT (SECOND) OF TORTS § 222A(1) (1965).

126. *Id.* § 220; KEETON, *supra* note 81, § 14, at 85.

127. 763 F. Supp. 1473, 1493-94 n.28 (D. Minn. 1991), *aff'd, remanded sub nom.* American Computer Trust Leasing v. Boerboom Int'l, Inc., 967 F.2d 1208 (8th Cir. 1992), *cert. denied*, 113 S. Ct. 414 (1992).

128. *Id.* at 1493-94 (quoting Mondt v. Sexter Realty Co., 293 N.W.2d 376, 377 (Minn. 1980)). Minnesota requires that the property involved be "produced by and grown upon land"; thus, taking by deactivation did not fall within the statute. *Id.* at 1493.

129. MINN. STAT. ANN. § 332.51 (West Supp. 1993) (providing that "[t]here can

Inc. v. Cyber Promotions, Inc.,[130] the court enjoined the defendants from sending junk e-mail to the plaintiff's e-mail addresses because the defendant's conduct, which continued after repeated requests to stop, constituted actionable trespass to chattel under Ohio law. Electronic signals were sufficiently tangible in depriving CompuServe of the use of its chattel, even though its physical condition was not impaired.[131] The court followed the reasoning in *Thrifty Tel, Inc. v. Bezeneck*,[132] where the plaintiffs were found guilty of trespass to chattel in California for using unauthorized computer code to gain computer access.[133]

Disabling code that locks up a computer system or application would therefore probably support an action for either conversion or trespass to chattels.[134] In *Clayton X-Ray Co. v. Professional Systems Corp.*,[135] the software provider was found liable for conversion of purchaser's system after the purchaser refused to pay for the software.[136] The court reasoned that the provider's installation of the disabling device, under the guise of performing a system upgrade, constituted conversion because "[t]he effect of the lockup was to prevent Clayton's access to the records of its business."[137] If expressly provided for in an agreement, these self-help remedies are generally governed by contract law and are likely both legal and effective. However, courts may be unlikely to hold that self-help disabling devices are valid unless a contract provides for these

---

be no nuisance if a party cannot show an injury stemming from an interest in land."). Thus, the court held that "the use of a computer system is not the type of property protected by the statute." *American Computer Trust Leasing*, 763 F. Supp. at 1494.

130. 1997 WL 109303 (S.D. Ohio Feb. 3, 1997).

131. *Id.* at *6-7.

132. 46 Cal. App. 4th 1559 (1996).

133. *Id.* at 1567.

134. Robbins, *supra* note 7, at 26.

135. 812 S.W.2d 565 (Mo. Ct. App. 1991).

136. *Id.* at 567.

137. *Id.*

risks.[138] In *Franks & Sons, Inc. v. Information Solutions, Inc.*,[139] the court enjoined the software provider from executing its disabling device, reasoning that because the provision was not a part of their agreement, it was a "surprise in their product which chills the functioning of any business whose operation is a slave to a computer."[140] Damages from these self-help devices may include not only the customer's contracts with third parties, but also unrelated data which may be unforeseeably affected.[141]

2. *Non-intentional torts.*—Negligence could arise from failure to exercise reasonable care to detect or warn a user of a virus that may have been overlooked or inserted into deliverable software.[142] ISPs or BBS operators may also be liable for negligence if they should be aware of a virus transmitted through their systems.[143] Although employers may be vicariously liable for employee negligence within the scope of employment, liability for *intentionally* releasing a virus is confined to the employee, as in *Brandl*.[144] However, liability might lie in such a case where an employer negligently failed to utilize appropriate virus scanning mechanisms in "proofreading" the software before its release.[145]

---

138. Mary L. Beyer, *Managing the Risk of Virus Liability*, 10 COMPUTER LAW 22, 23 (Dec. 1993). *See also U.C.C. 2B (Draft)* § 2B-312, (last official draft Sept. 25, 1997) <http://www.law.uh.edu/ucc2b/092597/092597_2b.html> (permitting restraints that are consistent with the agreement); *id.* § 2B-716 (governing self-help restraints used in the event of breach). Any restraint unauthorized by sections 312 and 716 is considered a virus. *Id.* § 2B-311(a).

139. No. 88-C-1474-E, 1988 U.S. Dist. LEXIS 19356, at *1-3 (N.D. Okla. Dec. 23, 1988).

140. *Id.* at *3.

141. Beyer, *supra* note 138, at 23.

142. *See* Lyman, *supra* note 29, at 626. Violation of a criminal statute might constitute evidence of negligence per se in those jurisdictions permitting civil actions under the statute, or by analogy in other jurisdictions. *Id.* at 623.

143. *See supra* notes 99-106 and accompanying text.

144. North Tel., Inc. v. Brandl, 179 B.R. 620, 623 (Bankr. Minn. 1995).

145. *See, e.g.*, Pettengill v. Booth Newspapers, Inc., 278 N.W.2d 682, 684 (Mich. Ct. App. 1979) (rejecting defendant newspaper's theory that a "phantom writer" who intentionally inserted defamatory statements for publication into newspaper's automated publishing system was responsible for defendant's negligence).

a. Negligent misrepresentation.—To avoid preempting contractual issues, courts distinguish negligence claims from contractual claims, which include an implied duty of reasonable care.[146] When malevolent software is mass-marketed, licensed, or sublicensed from third parties the software provider could be held liable for negligent misrepresentation causing economic losses.[147] Generally,

> [o]ne who, in the course of his business . . . supplies false information for the guidance of others in their business transactions, [is] subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.[148]

In *Rosenstein v. Standard & Poor's Corp.*,[149] the court found that Standard & Poor's ("S&P") owed a duty sufficient to create a claim

---

146. RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENSES, LIABILITIES (2d ed. 1996) § 10.13[1] at 10-35. One approach distinguishes between misfeasance of contract obligations and nonfeasance thereof, where negligence standards do not apply. *Id.* A second approach suggests that tort law governs defendant's conduct outside the bargain consented to by the parties. *Id.* at 10-35, 10-36. A third approach considers the nature of injury, where economic consequences of a contract are part of the bargain. *Id.* at 10-36.

147. *Id.* The circuits are split regarding the validity, and thus enforceability, of contracts for mass-produced software known generally as shrinkwraps (or webwraps as used in Internet transactions). The Seventh Circuit recently held a shrinkwrap license valid in *ProCd, Inc. v. Zeidenberg*, 86 F.3d 1447, 1453 (7th Cir. 1996), in contrast to earlier decisions which rejected the enforceability of shrinkwraps. *See, e.g.*, Step-Saver Data Sys., Inc. v. Wyse Technology, 939 F.2d 91, 105 (3d Cir. 1991) (refusing to incorporate into parties' contract additional terms detailed in box-top license if incorporation materially alters parties' agreement); Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 270 (5th Cir. 1988) (finding unenforceable a provision in computer programmers' license agreement prohibiting the decompilation or dissassembly of its program); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 763-64 (D. Ariz. 1993) (finding that contract was formed when buyer opened shrinkwrap on live version of software rather than when seller shipped the goods). For a more thorough discussion of shrinkwrap licenses, see generally Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995). *See also U.C.C. 2B (Draft)* § 2B-313 (last official draft Sept. 25, 1997) <http://www.law.uh.edu/ucc2b/092597/092597_2b.html> (recognizing mutual contractual obligations to exercise "reasonable care" in excluding viruses, which departs from current law permittting disclaimers). What constitutes reasonable care varies with the facts and circumstances of each transaction. However, the new UCC expressly excludes on-line and tangible mass-market transactions from provision (c) which allows disclaimer of liability for viruses. § 2B-313, Reporter's Notes 2-4.

148. RESTATEMENT (SECOND) OF TORTS § 552 (1976).

149. 636 N.E.2d 665 (Ill. App. Ct. 1993).

of negligent misrepresentation. The court reasoned that although S&P Indexes had become salable products, the Index did not shed its character as an important source of economic information.[150] However, S&P's disclaimer of its duty to provide accurate information contractually relieved it of its risk for the loss.[151] Software service providers may be held to have a similar duty, but may only expressly disclaim this potential liability to a limited extent.[152]

Even when liability is found, however, a virus victim may not be able to recover economic losses. In *Apollo Group, Inc. v. Avnet, Inc.*,[153] the court refused to except negligent misrepresentation from the economic loss rule in a third-party suit, as other courts have for negligent delivery of contracted services, because it felt that this sale of computer hardware was not a service.[154] The court in *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*[155] rejected the claim that the rule did not apply to a customized computer system which included software, hardware, and a maintenance agreement.[156] The court recognized that the exception had only been applied where defendants were professionals held to a higher standard of care in supplying professional services.[157]

With most performance-related claims regarding misrepresentation, courts appear to refuse parties' attempts to skirt the provisions of the bargains into which they entered.[158] However, it is arguable that courts would be more receptive in the case of virus infections

---

150. *Id.* at 667-68.

151. *Id.* at 672.

152. *See* sources cited *supra* note 147.

153. 58 F.3d 477 (9th Cir. 1995).

154. The court noted that there was no consensus among jurisdictions having addressed the issue and distinguished previous Arizona authority permitting recovery in tort where lack of privity precluded a contractual remedy, thus rendering commercial law an inadequate framework in which to resolve claims. *Id.* at 480. *Cf. In re* Illinois Bell Switching Station Litig., 641 N.E.2d 440, 444 (Ill. 1994) (finding no liability where plaintiffs' disruption of service was not damages arising from personal injury or "other property," and thus was not recoverable).

155. 53 F.3d 195 (8th Cir. 1995).

156. *Id.* at 198.

157. *Id.*

158. Joseph P. Zammit, *Recent Developments in Computer-Related Misrepresentation*, C601 ALI-ABA 75, 77 (discussing the practical limits for misrepresentation claims for software).

because parties would not generally agree to defective services which would damage other portions of their business enterprise.

b. Third party and products liability.—Providers of computer system products, such as security software, and potentially providers of computer services, may face liability if they do not provide adequate security mechanisms to ensure that their products present no unreasonable risks from viruses.[159] For example, Java, the Internet programming language developed and distributed by Sun Microsystems,[160] has been found to be susceptible to virus attacks.[161]

Few courts appear to allow recovery for negligent design of virus software to third parties, especially when damages are limited to economic losses.[162] The court in *Edwards v. Honeywell, Inc.* [163] concluded that an alarm service company had no duty to a third-party fireman, rejecting his claim that the service was negligent in failing to notify the fire department of the fire in a timely fashion; this failure, he claimed, resulted in his fall through a floor that had been weakened by the fire.[164] The court reasoned that the provider of the alarm service had no knowledge of the risk of a fire, no practical ability to reduce that risk, and no knowledge of the risk to the firemen summoned to extinguish it.[165] The costs of providing alarm service should be market-driven because imposing a duty on the service provider would outweigh the administration costs.[166]

New security products have been described as "close to the level of 'bullet-proof'" or "hacker-proof," and pose the issue of an appropriate application of products liability—questions remain as to

---

159. *See* Lyman, *supra* note 29, at 632-33 (suggesting that products liability could in theory apply to software providers, but that virus-infected programs are not generally considered unreasonably dangerous).

160. *Java White Papers* (last modified Feb. 2, 1998) <http://www.java.sun.com/docs/white/index.html>.

161. *Deadly Black Widow on the Web: Her Name is JAVA* (May 5, 1996) <http://www.westol.com/~informer/guide/java.html>.

162. *See, e.g.*, Robbins, *supra* note 3, at 25 (discussing tort liability for computer viruses).

163. 50 F.3d 484 (7th Cir. 1995).

164. *Id.* at 490-92.

165. *Id.* at 490-91.

166. *Id.* at 491.

whether these representations would be judicially enforceable.[167] An illustrative exmple is Sun Microsystem's Java, billed as a "robust, secure, architecture-neutral . . ." language for the Internet that is implemented through platform-independent applets, which later was shown to be vulnerable to several types of security breaches.[168]

Santor v. A & M Karagheusian, Inc.[169] represents the leading authority for the minority view, which permits tort action in negligence or strict tort liability to the "disappointed purchaser" who has suffered property loss where the property harmed is the product itself, and where there is no contract between the parties.[170] However, this view requires damage to the product itself and is unlikely to apply unless a virus were to erase the defective software in which it arrived.

Imposing strict products liability, or liability without fault, on transactions in goods shifts the risks to those better equipped to bear the liability as a mechanism to prevent accidents.[171] Strict liability originally was limited to items "unreasonably dangerous" to the consumer,[172] and the requirement for physical damage generally limited claims to those involving a risk of personal injury to foreseeable plaintiffs. Most courts permit recovery for damage only to the defective product itself, and liability can be disclaimed if negotiated and unambiguous.[173]

The *Winter* court realized that software is distinguishable from information because it functions.[174] Even if intangible, software's

---

167. Rustad & Eisenschmidt, *supra* note 3, at 218 n.31-32.

168. *Java White Papers* (last modified Feb. 2, 1998) <http://www.java.sun.com /docs/white/index.html>.

169. 207 A.2d 305, 306 (N.J. 1965).

170. *Id. See* D'Angelo, *infra* note 219, at 592-99 (describing both the minority and majority views); *cf.* Seely v. White Motor Co., 403 P.2d 145, 155 (Cal. 1965); East River Steamship Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 870 (1986) (supporting the majority view in denying recovery in strict tort liability where the only economic loss is in the product's failure to perform to buyer's expectations). *See also* Lang v. General Motors Corp., 136 N.W.2d 805, 810 (N.D. 1965) (holding that a purchaser has a cause of action under negligence for a defective truck for lack of due care in manufacturing against a manufacturer who promotes a product in the stream of commerce).

171. KEETON, *supra* note 81, § 98, at 692-93.

172. RESTATEMENT (SECOND) OF TORTS § 402A (1976).

173. KEETON, *supra* note 81, § 101, at 709.

174. Pamela Samuelson, *A Manifesto Concerning The Legal Protection Of Computer Programs*, 94 COLUM. L. REV. 2308, 2316-18 (1994).

intended function is to execute system commands that control hardware, the malfunction of which would cause foreseeable injuries. The court in *Vandermark v. Ford Motor Co.*[175] allowed a claim for strict liability when injuries resulted from an accident caused by a brake malfunction. If brake malfunctions subject a car manufacturer to strict liability, it is conceivable that a provider of anti-lock brake software, firmware, or hardware would be subject to the same liability if it were a cause in fact of injury.[176]

Liability for Internet software products is tenuous but appears to have some merit where personal injury is at stake. In *Winter v. GP Putnam's Sons*,[177] the court held that a publisher was not liable for injuries suffered after relying on information in a book, because the plaintiff was not injured by the intended use of the product —reading.[178] The publisher also had no duty to ensure the accuracy of the information contained within the book.[179] The court distinguished the book from the airport instrumental approach charts relied upon in *Aetna Casualty & Surety v. Jeppeson & Co.*,[180] which subjected the publisher to strict liability, because the intended function of the charts was to safely guide aircraft.[181] The *Winter* court did not draw a bright line between the physical product and the intangible ideas represented, but commented in dicta that software which "fails to yield the result for which it was designed" may be a product that involves information but falls within the purview of product liability.[182]

---

175. 391 P.2d 168, 171 (Cal. 1964) (en banc).

176. *See generally* Sparacino v. Andover, 592 N.E.2d 431, 434 (Ill. 1992) (finding vendor not liable for a software system that was not dangerous as assembled, but suggesting that because installation of the software created a dangerous condition, installer may have had a duty to warn).

177. 938 F.2d 1033 (9th Cir. 1991).

178. *Id.* at 1037.

179. *Id.*

180. 642 F.2d 339 (9th Cir. 1981).

181. *Id.* at 342-43.

182. *Id.* at 1036; *see also* Chatlos Sys., Inc., v. Nat'l Cash Register Corp., 479 F. Supp. 738, 743 (D.N.J. 1992) (holding software retailer liable for breach of express warranties and the implied warranty of fitness for the sale of software that did not perform as warranted). However, courts have been slow to develop products liability against vendors of software, probably because historically software was more a service than a product. Rustad & Eisenschmidt, *supra* note 3, at 259.

ISPs provide a distribution service to which traditional strict liability does not apply, which presents an additional challenge in analysis.[183] However, a minority of jurisdictions permit recovery under the doctrine for services; the inquiry appears to be whether the service provider "is the kind of enterpriser who ought in the public interest to be strictly accountable for harm resulting from the defects in things transmitted in the course of rendering services."[184] Moreover, mass-supplied Internet service may be distinguishable from the service transactions originally thought inappropriate for claims under strict liability.[185]

3. Contractual claims.—The first case addressing whether damage to system data would trigger product liability was *Transport Corp. of America, Inc. v. IBM.*[186] Transport Corporation of America ("TCA") purchased an IBM computer system with a daily backup function. Its disk failed, destroying the data and rendering the system inoperable until replacement. The court denied tort recovery for both negligence and strict liability because Minnesota law does not permit recovery for purely economic loss.[187] TCA's argument that destruction of its data constituted damage caused to "other property" was refuted as a matter of law.[188] The court held that the data and the system were integrated, and under Minnesota law, "where a defect in

---

183. KEETON, *supra* note 81, § 104A, at 719-20. Doctrinal policy has not generally applied to services. *See* Nimmer, *supra* note 146, § 10.14[2][a], at 10-42-10-43. This policy suggests that selling services to provide guidance for others should subject service providers only to reasonable care and competence, not infallibility. *Id.* Further, services are not usually provided in the context of mass marketplace, which involves distant customers for whom it would be unfair to trace the article they used to the original manufacturer and to pinpoint the act of negligence "remote" to their knowledge. *See id.*

184. KEETON, *supra* note 81, § 104A, at 721. *See, e.g.*, Melody Homes Mfg. Co. v. Barnes, 741 S.W.2d 349, 355 (Tex. 1987) (stating that mobile home manufacturer has implied duty to reasonably repair defects under implied warranty).

185. *See* Nimmer, *supra* note 146 § 10.14[2][a], at 10-42-10-44 (suggesting that some mass-marketed software products may be distinguishable from those person-to-person service contracts that are traditionally exempted from the doctrine). ISPs can likely bear the costs and distribute them among consumers. *See* KEETON, *supra* note 81, § 98, at 693 (discussing general policies underlying the doctrine of strict liability).

186. 30 F.3d 953 (8th Cir. 1994).

187. *Id.* at 956-57.

188. *Id.* at 957.

a component part damaged the product into which that component was incorporated, economic losses to the product as a whole were not losses to 'other property.'"[189] Further, because tort claims are only available where the nature of the defect or loss is not contemplated by the contracting parties, the court found that TCA had no claim in tort, but was limited to UCC remedies.[190]

The court in *Sparacino v. Andover Controls Corp.*[191] held that the manufacturer of a computerized energy management system was not liable for a teacher's injuries caused by chlorine gas when the system shut off an exhaust fan used to vent the gas.[192] There was no defect in the system, because it had operated the way it was programmed. Further, since the dealer controlled some of the system programming, the system was not defective as assembled, but was potentially defectively installed. The court then reasoned that the manufacturer had no duty to warn of all possible risks associated with the system, only those objectively reasonable.[193]

Because online transactions are likely to include several contractual limitations, virus victims may be barred from a claim based in tort.[194] However, courts must assess the validity of these contracts, which effectively trade a victim's entire computer system integrity as consideration for the privilege of access, or use of one computer program.[195]

D. *Causation*

1. Cause in fact.—Establishing "but for" cause for both the virus and its source will likely be difficult because networked systems are

---

189. *Id.*

190. *Id.* at 958.

191. 592 N.E.2d 431 (Ill. 1992).

192. *Id.* at 436.

193. *Id.*

194. ISPs and software providers will likely employ disclaimers for their services and products. *See Introduction to the Internet, in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES, 1, 4 n.10 (Joseph F. Ruh ed., 1996). However, these may be subject to new developing standards. *See, e.g.*, sources cited *supra* note 147.

195. The validity of shrinkwrap or webwrap licenses as contracts of adhesion is still in question. *See* sources cited *supra* note 147.

accessed simultaneously by many different systems, users and programs. Thus, the consequences of each transaction will be a function of the nature of the virus's entry to the system, latency effects, and the sophistication of the rogue code in evading detection. Systems that employ audit trail capabilities to both detect the entry of rogue programs and log system transactions will fare better in pinpointing the culprit, but once external to a computer or network, tracing the path of a virus across the Internet becomes proportionally complex, depending on each service provider's tracking mechanisms.

Latency presents problems with determining causality from system failure or damage to data. The failure of an anti-viral program to detect a virus already resident on a system, but in its dormant state, may give the impression that the virus's entry was subsequent to the virus detection program's failure. Rogue programs that cause slight damage over time can be analogized to exposure damage in mass torts: although exposure may have been a singular event, damages caused by an initial exposure over time become inseparable from multiple sources, similar to aging or other disease processes.[196]

2. Proximate cause.—Courts that permit recovery of economic damages for negligence appear to treat the issue as one of proximate cause or as duty owed to a class of foreseeable plaintiffs.[197] Some jurisdictions permit recovery for economic damages which flow from proximately caused damages to physical property,[198] while others permit recovery from proximately caused economic damages with no

196. *See* Lyman, *supra* note 29, at 626 (discussing latency effects of computer viruses).

197. *See* John M. Palmeri & Monty L. Barnett, *The Continuing Vitality of the Economic Loss Rule*, 31 LAND & WATER L. REV. 757, 761-62 (1996) (discussing some exceptions to the general economic loss rule). *See, e.g.*, A.E. Inv. Corp. v. Link Builders, Inc., 214 N.W.2d 764, 769 (Wis. 1974) (allowing tenant to maintain negligence action against architect and builder for defective building construction design that resulted in tenant's economic losses, even though the parties were not in privity); People Express Airlines, Inc., v. Consolidated Rail Corp., 495 A.2d 107, 118 (N.J. 1985) (holding that defendants could be liable to particularly foreseeable plaintiffs for their reasonably anticipated losses); J'Aire Corp. v. Gregory, 598 P.2d 60, 64 (Cal. 1979) (holding that contractor could be liable for lessee's foreseeable economic losses).

198. Palmeri & Barnett, *supra* note 197, at 762.

physical property damage.[199] It is reasonable that where computer data damaged by a virus attack is construed as physical property damage, economic harms flowing from loss of the victim's data, operational system, human resources, and ensuing breaches of contract are likely foreseeable in the event of a viral infection.

Networked systems present a complex inquiry into proximate cause between the source of the virus and the injury, similar to that for causation in fact. The Internet consists of many independent actors who may introduce intervening causes, which are generally unforeseeable, independent of the wrongful act or omission, and adequate to bring about the injurious result.[200] Service providers' unknowing transmission of rogue code would likely not constitute an intervening cause that would limit the liability of the original tortfeasor who released the virus.[201] However, it stands to reason that a service provider's *knowing* transmission of a viral code may constitute an intervening cause, or contributory negligence. Generally, though, on-line service providers have little control over materials available to be downloaded from the Internet. CompuServe, for example, provides notices to users as they pass through its gateway to the Internet that disclaim CompuServe's control or warranty of the data.[202]

Sparacino v. Andover Controls Corp.[203] illustrates a case in which an intervening cause might supersede a manufacturer's liability for negligence in delivering software products.[204] Had the manufacturer

---

199. *See* Edward L. Raymond, Jr., Annotation, *Business Interpretation, Without Physical Damage, as Actionable*, 65 A.L.R. 4th 1126, 1132-34 (1989) (finding courts used both proximate cause and duty to foreseeable plaintiffs to hold parties liable to purely economic losses).

200. KEETON, *supra* note 81, § 44, at 304.

201. *See* Religious Tech. Ctr. v. Netcom, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (suggesting that service providers are not liable for copyright infringement without some knowledge the activity has arisen on its computers).

202. The notice reads: "It is your responsibility to determine that a file contains information or programs you want, that it will work on your equipment, that you have rights to copy and use the information, and that it does not contain any virus or other potentially damaging side effects." *Introduction to the Internet, in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES 1, 4 n.10 (Joseph F. Ruh ed., 1996).

203. 592 N.E.2d 431 (Ill. 1992) (finding gas ventilation system manufacturer not liable for injuries caused after the system shut off the exhaust fan).

204. *Id.* at 435.

been negligent in programming its ventilation software, the dealer's subsequent negligence in failing to control or install it properly, or to warn the purchaser likely would have superseded the manufacturer's negligence. Similarly, most jurisdictions would generally find that were a consumer to misuse a software product in an unforeseeable way, a claim for products liability would be severed.[205]

E. Defenses

Tort liability may not lie where there is privity between the parties and they have allocated the risks of transaction between themselves.[206] Courts may generally defer to a contract or license that expressly provides for virus indemnity, limitations for remedies, and liability for consequential damages, or allocates the burden of proving that damages were caused by a provider.[207] It is unclear whether a disclaimer will be successful in cases involving virus attacks in the case of mass-distributed software or over the Internet, where a user usually has no other alternatives, because the courts appear to be divided as to the validity of these contracts.[208]

It is hardly reasonable to maintain that connecting to the Internet implies consent to intentional infection by rogue code, or a rebuttable presumption thereof. An excellent analogue for opening up a computer system to new software on the Internet is presented by a store owner's consent to public traffic within and in the vicinity of the premises. The proprietor is not presumed to consent to either criminal or tortious activity simply because he permits public traffic invitees on the premises.[209]

---

205. *See* KEETON, *supra* note 81, § 102, at 711 (stating that unforeseeable misuse of a product is a superseding cause even if the product was defective).

206. *See supra* notes 187-195 and accompanying text.

207. Beyer, *supra* note 138, at 23.

208. *See* Lemley, *supra* note 114, at 317-22 (discussing confusion in the current state of the law regarding validity of shrinkwrap licenses for mass-produced software). *See* sources cited *supra* note 147.

209. The traditional divisions of licensee, invitee, and trespasser, although abandoned in some states, hold the proprietor to various standards of liability and due care with respect to only "the part of the premises . . . open to him for the purpose which makes him an invitee." KEETON, *supra* note 81, § 61, at 424.

It follows that when a user connects to the Internet, she consents to access by the responding site only to that *part of her system required, for the purpose of the transaction*. That level of access is clearly violated when a virus is downloaded, because transfer of a virus would not be included in the transaction's purpose, nor would the user intend to permit violation of her entire computer's integrity from a virus infection.

The real issue thus lies in the realm of unintentional attacks. Reason dictates that if tort liability governs damages caused by virus infection, risks should be allocated equitably among those choosing to engage in electronic commerce. Risks of virus infections and the potential resulting harms are known in the industry. Where suppliers are liable for providing a technologically sound means for prevention of virus transmission, consumers and users of software or data should be held to a reasonable standard for preventing the negligent entry of a virus into their systems.

Thus, a user probably should be held contributorily negligent where he does not follow, at a minimum, the informal "reasonable" practices for overcoming common Internet system flaws. These practices include routine monitoring for rogue program activity, audit trails, back-ups, and maintenance for providing security to avoid virus infections or to minimize their consequences.[210] Similar minimal standards may include firewalls to monitor unauthorized access attempts at the entry points to an operating environment and virus detection software to prevent virus entry at the desktop, neither of which are employed by most corporations.[211]

Further, where a virus invasion has been detected, preventive measures to avoid future reinfection might be required to mitigate damages. Similarly, reporting an infection to those with whom a system might come into contact could be imposed as a minimal standard.[212]

Should products liability apply to software providers, legal rules should consider "state-of-the-art" defenses, because new viruses

---

210. Rustad & Eisenschmidt, *supra* note 3, at 222.

211. Gripman, *supra* note 106, at 171.

212. Unwanted publicity regarding a weakness in their computer systems discourages corporations from reporting, which impedes the promotion of awareness. Gripman, *supra* note 106, at 174.

continue to emerge.[213] Although the industry knows of the risks of virus attacks, every new virus takes advantage of another trap door, trojan-horse mechanism, or stealth device to evade detection, rendering software or service providers unable to guarantee a virus-free environment. Whether a state-of-the-art defense is applicable depends on whether the provider could know of a defect at the time the product is designed.[214]

Because the risk of new virus infection is known, it is arguable that products should warn a user of specific issues related to care in using the product. Although the risk of new viruses is known, it is likely technologically impossible to prevent infection from all new strains. Yet, despite this knowledge, products have been marketed as "hacker-proof" or secure.[215] These products might then require a warning that would adequately alert a user either to the product's limitations, or to its unavoidably defective nature. Anti-virus manufacturers might warn that their software should be utilized prior to connecting to the Internet, or that their software should be updated weekly to capture new virus-detection software that would increase the product's efficacy to its advertised "secure" status. A user who misuses the product then likely would diminish his recovery.[216]

F. Damages

Because only a minority of jurisdictions permit recovery for economic loss under various tort theories, the determinative inquiries will be (1) whether a virus caused harm to property and if so, (2)

---

213. The state-of-the-art defense refers to the level of scientific ability to discover or design out defects. *See* KEETON, *supra* note 81, § 99, at 700-01; *see also* Miyaki, *supra* note 84, at 134-35 (suggesting the defense might apply where manufacturers could not know of the risk involved and had tested the software to the extent conforming to scientific knowledge at the time of design).

214. *See* KEETON, *supra* note 81, § 99, at 700-01; *see also* Miyaki, *supra* note 84, at 134-35.

215. *Java White Papers* (last modified Feb. 2, 1998) <http://www.java.sun.com /docs/white/index.html>.

216. KEETON, *supra* note 81, § 102, at 76-78. *But cf. In re* Brandl, 179 B.R. 620, 625 (Bankr. Minn. 1995) (recognizing a loss to the owner of use or value of computer resources in trespass to chattels); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1015 (S.D. Ohio 1997).

computation of the value of the property. Generally, tort law provides no recovery for purely economic losses because they are best handled through contract law.[217] Damage to data, application software, or system software stored on disks or in memory that a virus eradicates has not historically been considered a loss in a property interest, but an economic loss not compensable without first flowing from a loss to property.[218]

Economic losses are generally defined as "the diminution in the value of the product because it is inferior in quality and does not work for the general purposes for which it was manufactured and sold."[219] They include "damages for inadequate value, costs of repair and replacement of the defective product, or consequent lost profits —without any claim of personal injury or damage to other property."[220] It is arguable that all computer data are not protectible property interests. For example, some data are electronic representations of documents that would be tangible if printed on paper, others are programs which perform functions, such as calculating payrolls. Damages to data interfere with the computer systems' ability to act as both a document repository as well as a functioning machine.

Predominant economic losses suffered by virus victims are lost operational time to return the computer system to the state it was before the attack, and any resulting lost business. The worst scenario might include personal injury resulting from malfunctioning computer programs impacted by malevolent code.[221] Widespread damages from

---

217. *See, e.g.*, Office Supply v. Basic/Four Corp., 538 F. Supp. 776, 792 (E.D. Wis. 1982) (holding that claim of negligent manufacture, design, installation and repair of a computer system failed to state a cause of action because of preemption by contract law).

218. *See, e.g.*, State of La. *ex. rel.* Guste v. M/V Testbank, 752 F.2d 1019, 1029 (5th Cir. 1985) (requiring injury to property with proprietary interest to recover for economic losses), *cert. denied*, 477 U.S. 903 (1986). *But see, e.g.*, People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 118 (N.J. 1985) (upholding negligence cause of action for economic losses where no physical injury was incurred).

219. Christopher Scott D'Angelo, *The Economic Loss Doctrine: Saving Contract Warranty Law From Drowning in a Sea of Torts*, 26 U. TOL. L. REV. 591, 591-92 (1995) (quoting Comment, *Manufacturers' Liability to Remote Purchasers for "Economic Loss" Damages—Tort or Contract?*, 114 U. PA. L. REV. 539, 541 (1966)).

220. *Id.* (quoting Casa Clara Condominium Ass'n v. Charley Toppino & Sons, *Inc.*, 620 So.2d 1244, 1246 (Fla. 1993) (quoting Note, *Economic Loss in Products Liability Jurisprudence*, 66 COLUM. L. REV. 917, 918 (1966))).

221. Rustad & Eisenschmidt, *supra* note 3, at 258.

a single virus event are difficult to assess, and are similar to those found in mass torts, with varying damage resulting from individual injuries, eggshell skulls, and latency effects.[222]

Because many state legislatures have drafted criminal statutes to recognize property rights in intangible computer data, a civil action in tort is more likely today.[223] Federal courts may also apply the same reasoning in virus cases as that used in computer misuse cases. For example, in *United States v. Sampson*,[224] the court noted that a computer is undoubtedly property, and that consumption of computer time and utilization of computer capacities were inseparable from the physical identity of the computer itself.[225]

One issue of property presented in *TCA v. IBM*[226] becomes more clear in networked systems. It is more reasonable to presume that defects which introduce losses into a network, whether internally or over the Internet, would be considered losses to "other property," and not damages to a product into which it was "incorporated," as the court reasoned in *TCA*.[227] One author has discussed the unique property issues manifested by cyberspace and has suggested several models for assessing boundary definitions for the Internet based on property denoting "not material things but certain rights"— more specifically, the right to exclude or to prevent access.[228] Another cautions against the indiscriminate characterization of information as property.[229]

---

222. *See supra* note 194.

223. *See, e.g.*, Safeco Title Ins. Co. v. Liberty Nat'l Title Ins. Co., 1989 WL 11079, at *5 (N.D. Ill. Feb. 9, 1989) (using provisions of previously repealed crime statute as basis for civil action).

224. 6 COMPUTER L. SERV. REP. 879, 880 (N.D. Cal. 1978) (reasoning that "conversion" as used in the statute could include misuse or abuse of property, and that appropriation of computer time and capacity fit within the contours of "use.").

225. *Id.*

226. 30 F.3d 953 (8th Cir. 1994).

227. *Id.* at 957.

228. Reeves, *supra* note 23, at 761-62.

229. *See generally* Pamela Samuelson, *Information as Property: Do Ruckelshaus and Carpenter Signal A Changing Direction in Intellectual Property Law?*, 38 CATH. U.L. REV. 365 (1989) (reviewing the potential impacts of Supreme Court case law classifying information as protective property).

Assessing the value of harm to intangible property is difficult.[230] A lodestar calculation might measure the effort required to restore the status quo ante by modeling the cost of the operational hours of the personnel required to detect and eradicate the virus, test the system, and restore the lost data. However, this does not encompass lost operational time, where, for example, the system might be calculating payrolls due or carrying messages to and from clients. Nor does it include lost operational time for personnel who have no access to system resources, or to clients who require system processing.

V. The Mass Tort Arena

The class action device removes duplicative transaction costs, and courts are likely to certify a class when it advances the judicial inquiry.[231] While judicial reticence to certify classes in mass tort actions has decreased over the years, the federal courts' stance on the issue of certifying classes in mass torts is unclear.[232] However, where no personal injuries are at issue, the courts' most serious concerns in certifying a class may not apply.[233] Mass property damage torts involve more homogeneity among class members and commonality of

---

230. Daly, *supra* note 95, at 464-65 (1993). Even where computer-stored data is recognized as "property," its value still requires assessment. *Id.* at 461-65.

231. The *Federal Rules of Civil Procedure* were promulgated with efficiency in mind. FED. R. CIV. P. 1.

232. John C. Coffee, *Class Wars: The Dilemma of Mass Tort Class Action*, 95 COLUM. L. REV. 1343, 1344-45 (1995) (discussing the trade-off between the high costs of duplicative litigation and an individual's right to control litigation involving personal interests). *See also* Greer Pagan, Comment, *Renewed Resistance?: The Federal Circuit Courts and the Problem of Mass Tort Class Actions*, 34 HOUS. L. REV. 807, 832-38 (discussing that recent court decisions and the proposed amendments to Rule 23 appear to limit the ability to certify a mass tort class action). Discussion regarding the proper litigation device and individual protections for mass torts is beyond the scope of this Note.

233. *See* Deborah R. Hensler, *Resolving Mass Toxic Torts: Myths & Realities*, 1989 U. ILL. L. REV. 89, 91-97 (1989) (describing several concerns a court may have when certifying a class, including the following: the individual's control of her litigation, the sanctity of the tort process, and the application of uniform class treatment to all individuals, especially the most seriously injured).

factual issues than torts with personal injuries, and thus they are more likely to be certified as class actions.[234]

A single virus released and distributed over the Internet which infects a number of victims appears to fit the salient features of mass tort. These characteristics include:

1. numerous victims against the same defendant(s);
2. claims arising from a single event or transaction;
3. questions of law and fact that are complex and expensive to litigate and adjudicate, frequently those scientific and technological in nature;
4. important issues of law and fact identical or common to groups or subgroups;
5. injuries widely dispersed over time, territory, and jurisdiction;
6. causal indeterminacy; and
7. disease and other injuries from long-delayed latent risks.[235]

A. Potential Parties to the Action

With some variation in substantive state laws, potential class plaintiffs include consumers, users, and bystanders of products or services who have suffered losses from viruses transmitted to them. Damages issues for all plaintiffs will be factually dependent and will vary with state law; thus, individual issues will likely predominate, rendering difficult any division of subclasses or class certification on this issue.

Class defendants would likely include those software or service providers liable for the virus infection, rather than judgment-proof individuals who create and distribute viruses. They likely also would

---

234. *See* Coffee, *supra* note 232, at 1345 n.2 (noting the greater homogeneity and commonality among class members present in property damage class actions and the greater frequency of certification for such classes); *In re* Masonite Corp. Hardwood Siding Prods. Liab. Litig., 170 F.R.D. 417, 418 (E.D. La. 1997) (denying certification based on *Castano* in a case over faulty siding).

235. ALI, ENTERPRISE RESPONSIBILITY FOR PERSONAL INJURY, REPORTERS' STUDY 389-91 (1991, vol. II).

include security software providers liable for anti-viral software that may have been defective or that failed to warn the plaintiffs.

B. Certification Issues

Generally, mass tort class certification is best handled under Federal Rule of Civil Procedure 23(b)(3),[236] where plaintiffs must satisfy the requisite elements of numerosity, typicality, commonality, and adequacy.[237] A Rule 23(b)(3) class certification requires that: (1) common questions of law and fact must predominate over individual questions; and (2) the class action must be superior to other available methods of adjudication.[238]

Further, the courts must balance four factors: (1) the plaintiff's interest in individual control over the litigation; (2) other pending litigation; (3) the desirability of concentrating the litigation in a particular forum; and (4) the difficulty of managing the proposed class.[239]

When these general requirements are met, the four subsequent factors rarely pose substantive obstacles.[240] The opt-out provision of Rule 23(b)(3) binds only those class members who wish to achieve economies of scale at the price of individual control, while freeing those interested to pursue individual suits.[241]

---

236. Pagan, *supra* note 232, at 811.

237. Rule 23(a) states:

> One or more members of a class may sue or be sued as representative parties on behalf of all only if (1) the class is so numerous that joinder of all members is impracticable, (2) there are questions of law or fact common to the class, (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class, and (4) the representative parties will fairly and adequately protect the interests of the class.

FED. R. CIV. P. 23(a).

238. FED. R. CIV. P. 23(b)(3).

239. *Id.*

240. Linda S. Mullenix, *Class Resolution Of The Mass-Tort Case: A Proposed Federal Procedure Act*, 64 TEX. L. REV. 1039, 1058 (1986).

241. *Id.*

Castano v. American Tobacco Co.[242] illustrates the difficulty with establishing the superiority of a class action over the problems of duplicative litigation and economic inefficiency encountered with individual suits. The court found it unlikely that individual litigation would result in negative value suits.[243] It suggested that "fairness may demand that mass torts with few prior verdicts or judgments be litigated first in smaller units" to establish general causation, typical injuries, and damages.[244] Further, class litigation cannot be a superior method of adjudication where immature torts introduce difficulty in assessing whether the predominance requirement of Rule 23 has been met.[245]

Courts can employ Rule 23(c)(4)(A) to certify limited purposes classes common to a smaller subclass of plaintiffs, including ascertaining liability and damages.[246] However, the (c)(4)(A) "limited issue class" must still meet the threshold (b)(3) requirements.[247] Further, this option is difficult in jurisdictions that do not encourage bifurcated trials in negligence lawsuits.[248] For example, the court in *Cimino v. Raymark Industries*[249] certified a Phase I class which encompassed the issues of gross negligence, punitive damages, and the state-of-the-art defense.[250] Phases II and III of the lawsuit addressed exposure and compensatory damages and proceeded as

---

242. 84 F.3d 734, 740 (5th Cir. 1996) (reversing the district court's certification of the class for core liability and punitive damages because variations in state law affect predominance and superiority). The court cited the lack of common claims, variations in state law, a reluctance to entrust the fate of an industry to a single jury, predominance of individual over common issues, and conflict between class member's interests. *Id.* at 740-50.

243. *Id.* at 748.

244. *Id.*

245. *Id.* at 740. A "mature" tort is one in which such a variety and volume of claims have been litigated, adjudicated, and settled by numerous litigants and juries such that unbiased estimates of claim values can be accessed. Peter H. Shuck, *Mass Torts: An Institutional Evolutionist Perspective*, 80 CORNELL L. REV. 941, 963 (1995).

246. Mullenix, *supra* note 240, at 1059.

247. *Id. See, e.g.*, Amchem Products, Inc. v. Windsor, 117 S.Ct. 2231 (1997) (subjecting settlement classes to threshold requirements of 23(b)).

248. Mullenix, *supra* note 240, at 1058-59.

249. 751 F. Supp. 649 (E.D. Tex. 1990).

250. *Id.* at 653.

consolidations of the roughly 2000 cases. Other courts certify classes where the facts establishing liability do not vary meaningfully.[251]

In *Central Wesleyan College v. W.R. Grace & Co.*,[252] eight common issues were certified among approximately 500 property owners.[253] The court followed *School District of Lancaster v. Lake Asbestos of Quebec, Ltd.*,[254] where class plaintiffs succeeded in their Rule 23(b)(3) class certification by extensively analyzing variances in products liability law across the jurisdictions, separating the law into four categories. The *Lake Asbestos* court noted that state law variations did not present insuperable obstacles to certification, because subclasses under different state law could be created.[255]

Severing issues to meet the predominance requirement must not result in the same issue being retried by different juries in violation of the Seventh Amendment.[256] Thus, damages should not be severed from the liability issue when that would require the defendant's negligence to be retried in front of a second jury. The court in *In re Rhone-Poulenc Rorer, Inc.*[257] held that certification would facilitate prosecution of more claims than would otherwise be brought and would pressure defendants to settle, despite the possibility that the plaintiffs' claims lacked legal merit.[258] The court rejected bifurcation, because it might subject the first jury's finding to reevaluation by successive juries who would determine issues such as comparative negligence and proximate cause.[259]

Tort litigation for virus infections may be distinguishable from *Castano* because the level of damages for most plaintiffs likely does not begin to approach that in the personal injury cases.[260] Thus, the superiority threshold may be easier to reach, for two reasons: (1)

---

251. Mullenix, *supra* note 240, n.176. *See, e.g.*, Vernon J. Rockler & Co. v. Graphic Enters., Inc., 52 F.R.D. 335, 336 (D. Minn. 1971) (certifying a class on the issue of whether a defendant made a material misrepresentation upon which the plaintiffs relied).

252. 143 F.R.D. 628 (D.S.C. 1992).

253. *Id.* at 642-43.

254. 789 F.2d 996, 1010 (3d Cir. 1986).

255. *Id.* at 1010.

256. U.S. CONST. amend. VII.

257. 51 F.3d 1293, 1302-03 (7th Cir. 1995).

258. *Id.* at 1298.

259. *Id.* at 1303.

260. *See supra* note 231 and accompanying text.

more plaintiffs would be likely to join a class rather than individually file suit; and (2) courts may be interested in setting a strong precedent, to counter the pernicious growth of the virus industry and its potential effect on commerce. However, given the courts' strong reticence to litigate immature torts in a class action forum, these factors likely will not tip the scales.

Rhone-Poulenc will likely also be distinguishable in litigation regarding virus-inflicted harms, as Posner indicated that the most compelling rationale for class certification—that individual suits are infeasible because each member's claim is "tiny relative to the expense of litigation"—was not present in the case.[261] Although many potential plaintiffs' claims may exceed the cost of litigation, in most cases damages will likely be too "tiny" to encourage filing individual suits. Further, it is arguable that negligence issues are separable and that comparative negligence issues can be tried by a second jury.[262]

However, the Rule 23(b)(3) commonality requirement may not be easily satisfied in the case where potential virus victims span many states and where their claims evidence a variety of causation factors. Thus, class certification might only be successful if victims were relatively concentrated geographically, because subclasses according to state could ostensibly be certified and bifurcated into core liability classes.

Some liability issues may be certifiable, including the vicarious liability of employers of an actor who negligently released a virus embedded in a software product. Vicarious liability is well-analyzed, and common issues are likely to predominate. Class certification regarding a software provider's liability for negligence in selling software infected with a virus may be similarly successful. Some state-of-the-art defenses may be certifiable. The issues are common to all plaintiffs or subclasses of plaintiffs; the determinative question will be whether courts will certify classes presenting issues of first impression.

---

261. *In re Rhone Poulenc*, 51 F.3d at 1299.

262. One commentator suggests, "This Seventh Amendment objection seems a weak argument, as a series of circuit court decisions have approved the use of successive juries to determine different questions, and Rule 23(c)(4)(A) explicitly contemplates use of such a procedure." Coffee, *supra* note 232, at 1440 (citing *Arthur Young & Co. v. United States Dist. Court*, 549 F.2d 686, 693 (9th Cir.), *cert. denied*, 434 U.S. 829 (1977)).

More difficult certification issues arise in the case of service providers, where a defendant's relationship varies widely with respect to the class plaintiffs. For example, an Internet service provider's knowing transmission of a virus would probably present liability issues of first impression that would be highly individualized and factually dependent, and thus difficult to certify.

Courts may be less reticent to certify classes in actions arising from damages caused by viruses because in the near-term, mass litigation will be limited to economic and property damage. However, they will probably hesitate to certify on manageability grounds: unlike most classic property issues, these tort issues are immature, and state substantive law provides little or no precedent as guidance. Further, liability and causation issues will be much more complex than in the case of a single tortfeasor such as the software provider in *Brandl*; on the Internet, a virus travels through many points of access and service providers to various users. Substantive state law issues such as comparative negligence and damages are probably individual, both with regard to the types and extent of harms.

VI. Conclusion

A viable and secure communications Internet will best be governed by a variety of legal and regulatory devices. Tort law can serve to channel development of industry security standards and expectations, as well as to deter further virus infections, but its immaturity currently renders it a relatively toothless alternative to criminal or market sanctions.

The tort arm of the legal Internet framework can be strengthened only by overcoming these issues:

1. Courts should continue to reevaluate the impacts of damages to computer data caused by viruses as losses of appropriate property interests. Although valuation of the property loss presents difficult problems, the alternative creates a vacuum in tort liability for damages caused by viruses.
2. Standards for industry conduct should more appropriately distribute risk. Minimum standards should balance a vendor's ability to disclaim liability with an adequate level of due care in designing software products and services. Online users should

employ security measures appropriate for their risk of loss when connecting to networks.

3. The Internet presents jurisdictional issues and wide variations in tort law which render substantive analysis in a global environment burdensome. Internet participants are faced with uncertainty in managing risk, hampering their strategies for conducting online business. As courts recognize security breaches and damages caused by viruses, they must harmonize new liability and causation issues for products liability, negligence, and intentional releases of viruses according to substantive tort law from a multitude of jurisdictions.
4. The class action is currently an untenable means of adjudicating Internet disputes over virus damage and will likely be rejected for failing to satisfy the manageability and superiority requirements of Rule 23. The absence of a class certification device for widespread viral damages could potentially undermine its deterrent effect on allocating risks, especially where individuals would not otherwise file suit.