UIC John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 4 *Computer/Law Journal - Winter 1992*

Article 5

Winter 1992

Civil Remedies for the Victims of Computer Viruses, 11 Computer L.J. 607 (1992)

Susan C. Lyman

NOTE

CIVIL REMEDIES FOR THE VICTIMS OF COMPUTER VIRUSES*

I. INTRODUCTION

In the past decade, the number of computers used for personal, business, and government use has rapidly increased.[1] Along with this increase, the world has looked on in horror as "deadly" programs have infected thousands of computers.[2] Known as "computer viruses,"[3] these programs are capable of destroying other programs, "crashing"[4] the user's computer system, and spreading to other computer systems through communication networks.[5]

As a result of a few highly-publicized computer viruses,[6] state legislatures and federal congressional leaders have begun to enact criminal laws that deal specifically with computer viruses.[7] Although criminal

---

* This article was awarded National First Place in the Seventh Annual Computer Law Writing Competition, co-sponsored by the Center for Computer/Law, Manhattan Beach, California and The John Marshall Law School, Chicago, Illinois. Reprinted by permission of Southwestern University School of Law, vol. 21:3.

1. Between 1981 and 1988, 42.5 million personal computers were sold in the United States. Approximately 20 million were in use in homes and 15.8 million in the workplace at the end of 1987. BUREAU OF THE CENSUS, U.S. DEP'T OF COMMERCE, STATISTICAL ABSTRACT OF THE UNITED STATES 1989 743 (1988).

2. In 1988, an estimated 250,000 United States computer users were affected by programs that could have potentially destroyed all the valuable data within their computer systems. Elmer-DeWitt, *Invasion of the Data Snatchers: A Virus Epidemic Strikes Terror in the Computer World*, TIME, Sept. 26, 1988, at 62.

3. A computer virus is a program that can spread from one computer to another and use each infected computer to propagate more copies. The virus program hides in the operating system and when another computer communicates with the infected host, the virus slips into the new system. Rheingold, *Computer Viruses*, WHOLE EARTH REV., Sept. 22, 1988, at 106.

4. "Crashing is defined as a 'system failure that requires at least operator intervention and often some maintenance before system running can resume.' Such a system failure often results in costly downtime for users." Note, *Computer Viruses: Is There a Legal Antibiotic?*, 16 RUTGERS COMPUTER & TECH. L.J. 253, 253 n.4 (1990) (citing DICTIONARY OF COMPUTING 86 (V. Illingworth 2d ed., 1986)) [hereinafter Tramontana].

5. *Id.* at 253.

6. *See infra* note 10.

7. *See infra* notes 39 and 55 and accompanying text.

punishment is an ideal way to deter computer "hackers"[8] from creating these programs, it provides little remedy to the victims who may have incurred millions of dollars in damages as a result of the viruses.[9] Victims of computer viruses may get little satisfaction from a criminal conviction if they are left with expensive clean-up costs or, in an extreme case, the cost of replacing an entire computer system.

This Comment will focus on a relatively new area of computer law: civil liability for computer viruses. First, this Comment will explore the remedies available under federal law and the difficulties that have arisen in applying the Computer Fraud and Abuse Act to a computer virus case.[10] Second, this Comment will focus upon the remedies available under state statutory law. A few states have criminal statutes that expressly deal with computer viruses and provide for civil remedies.[11] Such statutes allow victims to recover damages more easily than under any other type of state statute. Several other states have criminal statutes that do not mention computer viruses specifically, but do provide for civil remedies.[12] The remainder of state criminal statutes, however, are more difficult for the victims to rely upon as they do not specifically mention civil remedies and, in most cases, do not mention computer viruses. Third, this Comment will consider the use of state criminal statutes by analogy to the common law theory of negligence. This Comment will also explore particular common law tort claims which victims of computer viruses may resort to, such as trespass to chattel, conversion, negligence, and intentional interference with business relations. In one particular situation, the victim may even have a claim under the theory of products liability.[13] Finally, in addition to civil remedies, this Comment will discuss preventive measures available to all computer users such as tighter computer security, anti-viral programs, and insurance coverage.[14]

---

8. "Hackers" are skilled computer professionals or students with an intent to perpetrate an antisocial act of theft, embezzlement, or destruction. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 11 n.46 (1990) [hereinafter Branscomb].

9. The National Center for Computer Crime Data estimates that unauthorized access to American business computers during 1988 cost industry an estimated $555.5 million dollars. 135 CONG. REC. E2125 (daily ed. June 14, 1989) (letter by Rep. Herger).

10. United States v. Morris, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991). *See infra* notes 25-30 and accompanying text.

11. Only three states maintain both provisions: California, Texas, and Illinois. *See infra* note 56.

12. Such states include the following: Virginia, New Jersey, Missouri, Arkansas, and Delaware.

13. *See infra* notes 191-96 and accompanying text.

14. *See infra* notes 212-24 and accompanying text.

II. FEDERAL STATUTES

A. THE COMPUTER FRAUD AND ABUSE ACT

Currently, there is one federal law[15] and one legislative bill pending approval in the Senate[16] which address the problem of computer viruses. Congress passed the Computer Fraud and Abuse Act of 1986 (the Act)[17] to specifically address computer-related offenses. However, only two of the six crimes defined by the Act apply to computer virus offenders.[18] Section 1030(a)(3) of the Act prohibits conduct that interferes with the federal government's use of government computers.[19] This section requires that the perpetrator intentionally access the affected government computer.[20] Section 1030(a)(5) is somewhat broader than section 1030(a)(3); it proscribes altering, damaging or destroying information, or preventing authorized use of a "federal interest" computer.[21] Section 1030(a)(5) extends not only to computers used by or for the United States government,[22] but also to a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same [s]tate."[23] Like section 1030(a)(3), section 1030(a)(5) requires that the offender intentionally access the computer.[24] In many cases, this requirement will be difficult to prove because the virus programmer may not have intended to infect a computer that eventually becomes infected either through a network or electronic mail system.

In one particular computer virus case,[25] the perpetrator was convicted under section 1030(a)(5) of the Act for intentionally accessing a federal interest computer without authorization.[26] On November 2, 1988, Robert T. Morris created a virus[27] that disabled over 6,000 com-

15. 18 U.S.C. § 1030 (1988).

16. S. 1322, 102d Cong., 1st Sess. (1991).

17. 18 U.S.C. § 1030.

18. *Id.* § 1030(a)(3), (5).

19. *Id.* § 1030(a)(3).

20. *Id.*

21. *Id.* § 1030(a)(5).

22. *Id.* § 1030(e)(2)(A).

23. *Id.* § 1030(e)(2)(B).

24. *Id.* § 1030(a)(5).

25. United States v. Morris, 728 F. Supp. 95 (N.D.N.Y. 1989).

26. *Id.*

27. The program Morris created is technically referred to as a "worm." Such a program searches a computer system for idle resources and then disables those resources. By erasing information needed by the computer, the worm prevents the computer system from properly functioning. Denning, *The Science of Computing: Computer Viruses*, AM. SCIENTIST, May-June 1988, at 236.

puters around the world by using an electronic mail system.[28] Estimates of the damage caused by the virus have ranged from $96 million to $186 million based on labor costs to clear the memories of the computers and check the software for signs of recovery.[29] Morris' creation is one of the many programs that have caught the public's eye,[30] but few viruses have gained the same level of media and political attention.

Just recently, the Second Circuit dealt with the issue of intent as applied to computer virus cases brought under section 1030(a)(5).[31] Robert Morris appealed his conviction claiming that the government did not satisfy the intent requirement under the applicable section of the Act.[32] Morris asserted that the government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using the computer, thus causing damage.[33] The court looked to the legislative history of the 1986 amendment to the Act: "The Senate Report concluded that '[t]he substitution of an intentional standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another.' "[34] The court affirmed Morris' conviction by concluding that the intentional standard found in section 1030(a)(5) applied only to access and not to the resulting damage.[35]

The importance of this decision lies in the court's interpretation of intentional conduct under the Act. Although the Act does not specifically mention computer viruses, as the proposed bill does,[36] it clearly applies to the conduct of inserting a computer virus into federal computers. The difficulty arises in proving the requisite intent. Nevertheless, as the Second Circuit stated in its opinion, the only intent required is the intent to "access" a federal computer without authorization. Prosecutors can prove this intent by simply demonstrating that the per-

28. Schlender, *Computer Virus, Infiltrating Network, Shuts Down Computers Around the World*, WALL ST. J., Nov. 4, 1988, at B3.

29. Branscomb, *supra* note 8, at 7 (*citing Virus Cleanup: About $96 Million*, USA TODAY, Nov. 17, 1988, at 4B).

30. Kluth, *The Computer Virus Threat: A Survey of Current Criminal Statutes*, 13 HAMLINE L. REV. 297, 301-02 (1990) [hereinafter Kluth]; Branscomb, *supra* note 8, at 14-15. Other well known viruses include the "Universal Message of Peace" virus that infected approximately 100,000 Macintosh computers and the "Pakistani Brain" virus that infected hundreds of computers at the Universities of Georgetown, George Washington, Pittsburgh, Pennsylvania, and Delaware.

31. *Morris*, 928 F.2d at 504. The Second Circuit decided this case on March 7, 1991, as this Comment was being written.

32. *Id.* at 506.

33. *Id.*

34. *Id.* at 507 (*citing* 1986 U.S.C.C.A.N., at 2484).

35. *Id.* at 509.

36. *See infra* note 38.

son intended to and did disseminate the computer virus into a computer network that included governmental computers and that the person acted without authorization. The *Morris* decision has significantly strengthened the Act's application to computer virus cases since it has defined what type of conduct or intent falls within the Act.

B. THE COMPUTER VIRUS ERADICATION ACT OF 1989

Prior to *Morris*, it was extremely difficult to prosecute a computer virus case under the Computer Fraud and Abuse Act.[37] Because of these difficulties, Representative Herger introduced the Computer Virus Eradication Act of 1989[38] (the Virus Bill).[39] The Virus Bill would amend the Act by adding a section providing that it is a crime for any person to knowingly insert a harmful code into a computer or a computer program and then knowingly distribute that program to others.[40] Aside from adding a provision to the Act that specifically deals with computer viruses, the Virus Bill would also require "knowing" rather than "intentional" conduct.[41]

When Congress amended the Act in 1986, it changed the scienter requirement of section 1030(a)(5) from "knowing" to "intentional" in order to prosecute conduct that "evinces a clear intent to enter" a federal computer without authorization.[42] "Knowingly," as a mens rea standard, requires a lesser degree of proof because it can encompass a much larger area of impermissible conduct. As a Senate Report explains,

> [A] person is said to act knowingly if he is aware "that the result is practically certain to follow from his conduct, whatever his desire may be to that result." . . . "[I]ntentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective.[43]

Morris appears to have minimized the difference between the two mens rea standards, even though the difference between them is generally

---

37. The Computer Fraud and Abuse Act does not specifically deal with computer virus crime and requires an "intentional" rather than a "knowing" act before the statutory provisions can be satisfied. 18 U.S.C. § 1030(a)(3), (5).

38. H.R. 55, 101st Cong., 1st Sess. (1989).

39. The Virus Bill never came up for a vote in either the House or Senate in the first session of the 101st Congress. Kluth, *supra* note 30, at 305. However, the Senate is currently considering an amendment to the Act, entitled the Computer Abuse Amendments Act of 1991. S. 1322.

40. H.R. 55; 18 U.S.C. § 1030(a)(7)(A).

41. H.R. 55.

42. *See supra* note 34 and accompanying text.

43. S. REP. NO. 432, 99th Cong., 2d Sess. (1986) (citing *The Report on the Criminal Code*, S. REP. NO. 1396, 96th Congress, 33).

significant. The court held that the defendant need only intend to *access* the computer, not the resulting damage.[44]

However, as the *Morris* court pointed out in its opinion, to merely require a "knowing" standard would likely encompass "the acts of an individual 'who inadvertently stumbled into' someone else's computer file or computer data."[45] Although the Virus Bill would specifically include the knowing insertion of a computer virus into a computer system or network, this provision could possibly make careless conduct a crime. For example, a hacker may create a computer virus or worm, for his or her own personal enjoyment or for research purposes, and carelessly or inadvertently transmit the virus to another computer via electronic mail or an electronic bulletin board.[46] Although the transmission was careless, the fact that the hacker knew of the harm a virus could cause and still programmed it into a computer could be sufficient to satisfy the requirements of the Virus Bill.

The positive effect of the Virus Bill would be to punish anyone who *knowingly* creates a virus that intentionally *or* unintentionally harms another computer user. The negative effect would be to impose serious criminal penalties upon a person who did not intend to insert the virus into another computer or computer program, but who was merely careless or negligent. It is unclear what effect the *Morris* decision will have upon the enactment of the Virus Bill, but it is clear that both Congress and the courts, at least as to governmental computers, will require "intentional" access in a computer virus case.

In addition to adding more specific provisions regarding computer virus dissemination, the Virus Bill contains a provision permitting civil actions.[47] The provision states: "Whoever suffers loss by reason of a violation of subsection (a)(7) may, in a civil action against the violator, obtain appropriate relief. In a civil action under this subsection, the court may award to a prevailing party a reasonable attorney's fee and other

---

44. *See supra* note 35 and accompanying text. However, Senate Bill 1322, if enacted, would amend the Computer Fraud and Abuse Act and essentially overrule *Morris*. One of the amended provisions states that a person is guilty of a felony when he "knowingly causes the transmission of a program, information, code, or command to a computer or computer system" *and* "the person causing the transmission *intends that such transmission will damage, or cause damage to a computer* . . . ." S. 1322, § 1030(a)(5)(A)(i)(I) (emphasis added).

45. *Morris*, 928 F.2d at 507 (citing S. REP. NO. 432).

46. A computer bulletin board system is a computer program that simulates an actual bulletin board by allowing computer users to post messages, read existing messages, and delete messages. The messages exchanged may contain a wide variety of information, including stolen credit card numbers, confidential business information, and information about local community events. *See* Note, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439, 439-41 (1988).

47. H.R. 55; 18 U.S.C. § 1030(d).

litigation expenses."[48] The most important difference between the Act and the Virus Bill is the provision for civil remedies. In the *Morris* case, the prosecution estimated that *each* facility affected by the virus incurred costs ranging from $200 to more than $53,000.[49] Yet, none of the victims of Morris' virus could recover damages under the Act. However, under the Virus Bill, they might have been able to recover the costs incurred in restoring their computer systems and ridding the programs of the virus.

Although the Computer Fraud and Abuse Act has been used successfully in a computer virus case,[50] the Act lacks the specific statutory language found in the Virus Bill that would allow for more convictions of computer virus offenses. Additionally, unlike the Virus Bill, the Act does not permit civil actions against the perpetrator.[51] The Virus Bill, if enacted, would bring federal law up to date with many of the state statutes that do provide for civil remedies[52] and would enable the victims of computer viruses to recover damages for the losses incurred.

III. STATE STATUTES

A. CRIMINAL STATUTES THAT SPECIFICALLY PROVIDE FOR CIVIL ACTIONS

In order to deter computer hackers from creating viruses, however benign[53] they may be, almost every state has enacted criminal statutes that cover computer viruses.[54] The enactment of these laws is a rela-

48. H.R. 55. S. 1322 is more specific as to the civil remedies available, providing for compensatory damages and injunctive relief or other equitable relief. S. 1322, § 1030(c).

49. *Morris*, 928 F.2d at 506.

50. *Id.*

51. *See supra* notes 47-48 and accompanying text.

52. *See infra* note 56.

53. Gemignani, *What is Computer Crime, and Why Should We Care?*, 10 U. ARK. LITTLE ROCK L.J. 55, 65 (1987-88).

54. *See, e.g.*, ALA CODE §§ 13A-8-100 to 13A-8-103 (Supp. 1990); ALASKA STAT. §§ 11.46.200(a)(3), 11.46.740, 11.46.985, 11.46.990(1), 11.46.990(3) to 11.46.990(7) (Supp. 1990); ARIZ. REV. STAT. ANN. §§ 13-2316 (1989), 13-2301E (Supp. 1990); ARK. CODE ANN. §§ 5-41-101 to 107 (Michie Supp. 1991); CAL. PENAL CODE § 502 (West 1991); COLO. REV. STAT. §§ 18-5.5-101, 18-5.5-102 (1986 & Supp. 1989); CONN. GEN. STAT. ANN. §§ 53A-250 to 53A-261 (West 1985); DEL. CODE ANN. tit. 11, §§ 931-39, 2738 (1987 & Supp. 1990); FLA. STAT. ANN. §§ 815.01 to 815.07 (West Supp. 1991); GA. CODE ANN. §§ 16-9-90 to 16-9-95 (Michie 1990); HAW. REV. STAT. §§ 37-708-890 to 37-708-896 (1985); IDAHO CODE §§ 18-2201 to 18-2202 (1987); ILL. ANN. STAT. ch. 38, para. 15-1, 16D-3-4 (Smith-Hurd Supp. 1991); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (Burns Supp. 1991); IOWA CODE ANN. § 716A (West Supp. 1991); KAN. STAT. ANN. § 21-3755 (Supp. 1988); KY. REV. STAT. ANN. §§ 434.840 to 434.860 (Michie/Bobbs-Merril 1985); LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (West 1986 & Supp. 1991); ME. REV. STAT. ANN. tit. 71-a § 357 (West 1983 & Supp. 1990); MD. ANN. CODE art. 27, § 146 (Supp. 1990); MASS. ANN. LAWS ch. 266 § 30 (Law. Co-op Supp. 1990); MICH. COMP. LAWS ANN. §§ 752.791 to 752.797 (West 1991); MINN. STAT. §§ 609.87 to 609.89 (1987

tively recent event. "Before 1989, no state statute had mentioned computer virus by name and few, if any, made it a crime to release a computer virus."[55] Despite advances state legislatures have made regarding criminal penalties for computer viruses, relatively few statutes provide for civil remedies.[56]

1. *Statutes Specifically Addressing Computer Viruses*

a. California

The California Legislature recently enacted one of the most comprehensive computer crime laws specifically dealing with computer viruses.[57] Due to the increasing number of computer viruses sweeping the nation and the growing recognition that these viruses are not harmless programs, the California Legislature specifically included these programs in its amended computer crime statute.[58] California Penal Code section 502(b)(10) defines a "computer contaminant" as "any set of computer instructions that [is] designed to modify, damage, destroy, record,

---

& Supp. 1991); MISS. CODE ANN. §§ 97-45-1 to 97-45-13 (Supp. 1991); MO. ANN. STAT. §§ 569.093 to 569.099 (Vernon Supp. 1991); MONT. CODE ANN. §§ 45.2-1-1, 45-6-310 to 45-6-311 (1987); NEB. REV. STAT. §§ 28-1343 to 28-1348 (1989); NEV. REV. STAT. §§ 205.473 to 205.477 (1986); N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (1986); N.J. STAT. ANN. §§ 2A:38A-1 to 2A:38A-6 (West Supp. 1990); N.M. STAT. ANN. §§ 30-45-1 to 30-45-7 (Michie 1989); N.Y. PENAL LAW §§ 156.00 to 156.50 (McKinney Supp. 1988); N.C. GEN STAT. §§ 14-453 to 14-457 (1986); N.D. CENT. CODE §§ 12.1-06.1-01(3), 12.1-06.1-08 (Supp. 1991); OHIO REV. CODE ANN. §§ 2901.01, 2913.01 to 2913.04 (Anderson 1987 & Supp. 1990); OKLA. STAT. ANN. tit. 21, §§ 1951-56 (West Supp. 1991); OR. REV. STAT. § 164.377 (1990); PA. STAT. ANN. tit. 18 § 3933 (Purdon Supp. 1991); R.I. GEN. LAWS §§ 11-52-1 to 11-52-5 (Supp. 1990); S.C. CODE ANN. §§ 16-16-10 to 16-16-40 (Law. Co-op. 1985); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 43-43B-8 (Supp. 1991); TENN. CODE ANN. §§ 39-3-1401 to 39-3-1406 (Supp. 1990); TEX. PENAL CODE ANN. §§ 33.01 to 33.05 (West 1989 & Supp. 1991); UTAH CODE ANN. §§ 76-6-701 to 76-6-705 (1990); VA. CODE ANN. §§ 18.2-152.1 to 18.2-152.14 (Michie 1988 & Supp. 1991); WASH. REV. CODE ANN. §§ 9A.48.100, 9A.52.110 to 9A.52.130 (West 1988); W. VA. CODE §§ 61-3C-1 to 61-3C-21 (Supp. 1991); WIS. STAT. ANN. § 943.70 (West Supp. 1990); WYO. STAT. §§ 6-3-501 to 6-3-505 (Supp. 1988).

55. Kluth, *supra* note 30, at 307.

56. CAL. PENAL CODE § 502(e); ARK. STAT. ANN. § 5-41-106(a); N.J. STAT. ANN. § 2A:38-A-3; DEL. CODE ANN. tit. 11, § 939; CONN. GEN. STAT. §§ 53A-250 to 261; ILL. ANN. STAT. ch. 38, para. 160-310; TEX. PENAL CODE ANN. §§ 33.01-33.03; TEX. CIV. PRAC. & REM. CODE ANN. §§ 143.001-143.002 (West Supp. 1991); VA. CODE ANN. § 18.2-152.12. *See also* Bloombecker, *Cracking Down on Computer Crime*, STATE LEGIS., Aug. 1988, at 13.

57. CAL. PENAL CODE § 502(c). *See also*, Note, *An Overview of Recent Changes in California Computer Crime Laws*, 6 SANTA CLARA COMPUTER & HIGH TECH. L.J. 135 (1990).

58. CAL. PENAL CODE § 502(a). "In amending Section 502 to specifically criminalize the introduction of computer contaminants, the California Legislature recognized that computers are an integral part of society and that the phenomenon of computer virus contamination significantly threatens the reliability of those systems and data." DeGroot, *supra* note 57, at 136-37.

or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information."[59] In addition, section 502(b)(10) specifically includes "computer viruses" in its definition of a "computer contaminant."[60]

The actual provision that recognizes the criminal nature of a computer virus, however, is section 502(c)(8). This section makes it illegal for any person to "knowingly [introduce] any computer contaminant into any computer, computer system, or computer network."[61] In order for a conviction to stand under section 502(c)(8), a person must have "knowingly introduced"[62] a computer contaminant into a computer system or network.[63] Therefore, as long as prosecutors establish the intent to introduce the virus into a computer, they will meet the section 502(c)(8) requirement regardless of whether the person intended the resulting damage.

In addition to providing for fines and imprisonment,[64] the new legislation establishes civil remedies.[65] Section 502(e)(1) provides the following:

> In addition to any other civil remedy available, the owner or lessee of the computer . . . may bring a civil action against any person convicted [under Section 502(c)] for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer . . . was not altered, damaged, or deleted by the access.[66]

The only prerequisite for the civil action is that the defendant be convicted under section 502(c).[67] Moreover, the victim of a computer virus may pursue "any other civil remedy available."[68] This can be interpreted to mean that the legislature intended that the victim of a computer virus have several different civil avenues to pursue, rather than being limited to the remedy available under section 502(e). Additionally, the victim may also receive attorney's fees under section 502(e)(1).[69]

---

59. CAL. PENAL CODE § 502(b)(10).

60. Section 502(b)(10) of the California Penal Code defines computer viruses as "self-replicating or self-propagating [programs that] are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer . . . ." *Id.*

61. *Id.* § 502(c)(8).

62. *See supra* note 43 and accompanying text.

63. CAL. PENAL CODE § 502(c)(8).

64. *Id.* § 502(d).

65. *Id.* § 502(e)(1).

66. *Id.*

67. *Id.* § 502(c).

68. *Id.* § 502(e)(1).

69. *Id.* § 502(e)(2).

b. Texas

Texas is one of the few states, other than California and Illinois, to mention computer viruses specifically in its penal code[70] *and* provide for civil remedies under the statute.[71] Section 33.01 of the Texas Penal Code defines "computer virus" as

> an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself and to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.[72]

This definition of "computer virus" is very similar to the California definition. The primary difference between the two definitions is that California addresses "computer contaminants" that *include* computer viruses,[73] while Texas specifically addresses only "computer viruses."

The problem with the Texas statute is that it does not cover other types of programs that may afflict computer systems, such as worms.[74] Section 33.01(9) defines a computer virus as a program with the ability to "replicate itself" and attach to other programs.[75] This narrow definition excludes other potentially harmful programs from section 33.03(a)(6). Section 33.03(a)(6) states that "[a] person commits an offense if [he] intentionally or knowingly and without authorization from the owner . . . *inserts or introduces a computer virus* into a computer program, computer network, or computer system."[76]

Two interpretations will circumvent the narrow language of the statute. First, a court may interpret "computer virus" very broadly such that it encompasses all harmful programs regardless of the technical definitions of each program. Second, another subdivision of the statute may apply to the programs not specifically defined in section 33.01(9). Section 33.03(a)(1) states that it is an offense if a person knowingly or intentionally "damages, alters, or destroys a computer, computer program or software, computer system, data, or computer network."[77] By definition, a "worm" is a program that alters or destroys

---

70. TEX. PENAL CODE ANN. § 33.01(9).

71. TEX. CIV. PRAC. & REM. CODE ANN. § 143.001.

72. TEX. PENAL CODE ANN. § 33.01(9).

73. *See supra* notes 59-60.

74. "Computer 'worms' are malicious programs designed to move or 'worm' their way through a computer program to alter or destroy data." DeGroot, *supra* note 57, at 138 n.19.

75. TEX. PENAL CODE ANN. § 33.01(9).

76. *Id.* § 33.03(a)(6) (emphasis added).

77. *Id.* § 33.03(a)(1).

data,[78] a circumstance which brings it within the language of the statute.

Once a person circumvents the language of the Texas statute, or is the victim of a true "computer virus," that person may bring a civil action under section 143.001 of the Civil Practice and Remedies Code.[79] Section 143.001 allows for a civil cause of action "if the conduct constituting the violation [under Chapter 33 of the Penal Code] was committed knowingly or intentionally."[80] A person who establishes a cause of action is then entitled to actual damages and reasonable attorney's fees and costs.[81]

c. Illinois

Illinois is the third state that addresses computer viruses and provides for a civil remedy for any damages arising out of virus dissemination.[82] As amended,[83] Illinois' Computer Tampering section of its criminal code includes the insertion of a computer virus as an offense under section 16D-3.[84] Amended section 16D-3(a)(4) states the following:

> A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner . . . [i]nserts or attempts to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer . . . or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data . . . or that will or may cause [damage or] loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program."[85]

The amended section specifically defines what activity will constitute computer tampering; however, its language broadly encompasses all harmful programs, including worms and Trojan Horses[86] as well as computer viruses. The Illinois statute also employs a lesser mens rea

78. *See supra* note 74.

79. TEX. CIV. PRAC. & REM. CODE ANN. § 143.001.

80. *Id.*

81. *Id.* § 143.002.

82. ILL. ANN. STAT. ch. 38, para. 16D-3.

83. The amendments became effective January 1, 1990. *Id.*

84. *Id.* 16D-3(a)(4).

85. *Id.*

86. A Trojan Horse has been defined as a "desirable program which performs some useful function, such as logic, but which contains a parasite or viral infection within its login which is undetectable upon casual review." Branscomb, *supra* note 8, at 4-5 n.15 (*citing* Denning, *The Science of Computing: Computer Viruses*, 76 AM. SCIENTIST, May-June 1988, at 236).

standard since it requires that a person "knowingly" rather than "intentionally" insert a program.[87] Nevertheless, the statute does add that a person must "know" or "have reason to believe" that the program he knowingly inserts contains a harmful program.[88] This provision safeguards the person who may knowingly insert a program, but who does not know or have reason to believe that the program contains a computer virus. For example, a person may borrow a computer disk from an associate or friend, unaware that it contains a virus, knowingly insert the program into his computer, and then transmit the program via a bulletin board or electronic mail system. Under the Illinois statute, this person would not be subject to criminal prosecution.

The final provision added to the statute is section 16D-3(c). Section 16D-3(c) provides that "[w]hoever suffers loss by reason of a violation of subsection (a)(4) of this [s]ection may, in a civil action against the violator, obtain appropriate relief. In a civil action under this [s]ection, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses."[89] The provision for civil remedies is an important addition to the Illinois statute. By adding this provision, the legislature recognizes the economic harm that can arise when one disseminates computer viruses and allows the victim of such crime to receive compensation for his damages without the necessity of an expensive and difficult lawsuit.

2. *Other Criminal Statutes that Provide for Civil Remedies*

a. Connecticut

Under Connecticut law, the victim of a computer virus may also pursue a civil action.[90] However, unlike Texas, California, or Illinois, the Connecticut statute does not specifically address computer viruses. Yet, section 52-570b(c) does encompass damage caused by a computer virus. In an action for a computer-related offense, section 52-570b(c) provides that "any person who suffers any injury to person, business, or property may bring an action for damages against a person who is alleged to have violated any provision of section 53a-251."[91] Unlike the California provision,[92] a conviction under the relevant statute is not required before a victim of the crime can bring a civil action.[93] However,

87. *See* ILL. ANN. STAT. ch. 38, 16D-3.

88. *Id.*

89. *Id.*

90. CONN. GEN. STAT. ANN. § 52-570b(c).

91. *Id.*

92. CAL. PENAL CODE § 502(e)(1).

93. CONN. GEN. STAT. ANN. § 52-570b(f).

in Connecticut, a victim has the difficult burden of proving the requisite elements of the offense before the court may award damages.[94]

The Connecticut provisions that may encompass computer viruses include "[u]nauthorized access to a computer system,"[95] "[i]nterruption of computer services,"[96] and "misuse of computer system information."[97] In applying each of these provisions to a computer virus crime, the victim must prove either "intentional" *or* "reckless" acts.[98] Therefore, it may be easier for a victim to recover damages in a civil suit by showing only reckless behavior, rather than the more difficult intentional behavior. Assuming the victim can prove the requisite intent, section 52-570b allows him to recover actual damages, treble damages,[99] and reasonable attorney's fees and costs.[100]

b. Missouri

Missouri, like Connecticut, does not specifically mention viruses; however, it does address the problem of "damageless intrusions."[101] Missouri also added section 569.095 which addresses "[t]ampering with computer data," and makes it a crime if a person "knowingly . . . [m]odifies or destroys data or programs residing or existing internal to a computer, computer system, or computer network . . . ."[102] This new section would likely prohibit the insertion of a computer virus into a person's computer since such insertion would clearly constitute an unauthorized tampering under the Missouri statute if it modifies or destroys data within the affected computer system.

The Missouri statute also provides relief where a computer virus causes damage by either modifying or destroying data. The statute allows the victim of the computer access or tampering to "bring a civil action against any person who violates sections 569.095 to 569.099 . . . , for compensatory damages, including any expenditures . . . incurred by the owner to verify that a computer system . . . was not . . . damaged by the access."[103] In addition, similar to the other states, Missouri also allows the prevailing plaintiff to receive reasonable attorney's fees.[104]

---

94. *Id.* § 53A-251.
95. *Id.* § 53A-251(b).
96. *Id.* § 53A-251(d).
97. *Id.* § 53A-251(e).
98. *Id.* § 53A-251(b),(d),(e).
99. "Treble damages [shall be awarded] where there has been a showing of wilful and malicious conduct." *Id.* § 52-570b(c).
100. *Id.* § 52-570b(e).
101. MO. ANN. STAT. § 569.099.
102. *Id.* § 569.095.
103. *Id.* § 537.525.
104. *Id.*

c. Arkansas and Virginia

The Arkansas and Virginia statutes have virtually identical "computer trespass" and civil remedy provisions.[105] For example, Arkansas provides for recovery "for any damages sustained and the costs of the suit . . . [and] damages shall include loss of profits."[106] Under Arkansas' computer trespass provision, any intentional access, alteration, deletion, or disruption would violate the statute.[107] Thus, any damage sustained by reason of the violation is recoverable in a civil action under the Arkansas statute. Virginia has an identical civil remedy provision[108] that covers all damages caused by a "computer trespass" criminally punishable under section 18.2-152.4.[109] A "computer trespass" under the Virginia statute includes the intent to permanently or temporarily remove computer data, cause a computer to malfunction, or alter or erase computer data.[110] In both states, a violation of the applicable section is required before a victim may bring a civil action under the statute.[111]

A computer virus would likely fit within both trespass statutes since it can alter, remove, and erase data as well as cause a computer to malfunction. Both statutes require intentional conduct on the part of the perpetrator.[112] In contrast, none of the other states that provide for civil remedies requires intentional conduct, but instead apply the lesser knowingly standard or, as in Connecticut, only reckless behavior.[113] The higher standard of intent required in Arkansas and Virginia, coupled with the failure to specifically mention computer viruses in the statutes, may make computer viruses more difficult to prosecute. Furthermore, because these states also require that the perpetrator actually violate the statute, their laws make civil actions more difficult to win.

d. Delaware and New Jersey

The similarity between the Delaware and New Jersey statutes appears in the civil remedy provisions of each statute. Both New Jersey and Delaware allow a civil action without first requiring a violation of the criminal statute.[114] In Delaware, the section that would most likely

105. *See supra* note 56 and accompanying text.

106. ARK. CODE ANN. § 5-41-106(a).

107. *Id.* § 5-41-104.

108. VA. CODE ANN. § 18.2-152.12.

109. *Id.* § 18.2-152.4.

110. *Id.*

111. ARK. CODE ANN. § 5-41-106; VA. CODE ANN. § 18.2-152.12.

112. ARK. CODE ANN. § 5-41-104; VA. CODE ANN. § 18.2-152.4.

113. MO. ANN. STAT. § 569.095; CONN. GEN. STAT. ANN. § 53-261; CAL. PENAL CODE § 502(c); ILL. ANN. STAT. ch. 38, para. 16D-3; TEX. PENAL CODE ANN. § 33.03; DEL. CODE ANN. tit. 11, §§ 931-39; N.J. STAT. ANN. §§ 2A:38A-3a to 38A-3e.

114. N.J. STAT. ANN. § 2A:38A-3; DEL. CODE ANN. tit. 11, § 939.

apply to computer viruses is "[i]nterruption of computer services," which prohibits the intentional or reckless disruption or denial of computer services to an authorized user.[115] The most interesting aspect of the Delaware statute is that a victim may bring a civil suit against a person who *allegedly* violated any provision of the title.[116] Delaware Code section 939(f) reaffirms this provision by stating that "[t]he filing of a criminal action against a person is not a prerequisite to the bringing of a civil action under this section against such person."[117] Therefore, the victim of a computer virus may bring a civil cause of action under the statute without first seeking a conviction against the person. Under the statute, "the aggrieved person [may] recover actual damages . . . and treble damages where there has been a showing of wilful and malicious conduct."[118] The aggrieved person may also recover the reasonable costs and attorney's fees in bringing the action if he ultimately prevails.[119]

Similarly, under the New Jersey statute, *only* civil remedies are available to an aggrieved person. The provision dealing with computer-related offenses states the following:

> A person or enterprise damaged in business or property as a result of . . . [t]he purposeful or knowing, and unauthorized altering, damaging, . . . or destruction of any data . . . may sue the actor . . . and may recover compensatory and punitive damages and the cost of the suit, including a reasonable attorney's fee, costs of investigation and litigation.[120]

Not only do both Delaware and New Jersey *not* require a violation prior to bringing a civil action, but these states also authorize punitive damages for wilful or intentional conduct *without requiring a conviction under the statute*.[121] This means that these statutes significantly lessen the plaintiff's burden of proof. Rather than first requiring a criminal conviction, which requires a "reasonable doubt" standard, Delaware and New Jersey only require the plaintiff to prove fault by a "preponderance of the evidence." This type of provision allows the plaintiff to establish a knowing unauthorized access by a mere preponderance of the evidence.

Under California law, for example, the *state* would first have to prove a "knowing" unauthorized access beyond a reasonable doubt, *then* the plaintiff may sue for damages under the statute. Under the Califor-

115. DEL. CODE ANN. tit. 11, § 934.
116. *Id.* tit. 11, § 939(c).
117. *Id.* tit. 11, § 939(f).
118. *Id.* tit. 11, § 939(c).
119. *Id.* tit. 11, § 939(e).
120. N.J. STAT. ANN. § 2A:38A-3.
121. *Id.* § 2A:38A-3; DEL. CODE ANN. tit. 11, § 939(f).

nia statute, the plaintiff will most likely receive compensation by merely showing evidence of the conviction, but the defendant will get the benefit of a higher standard of proof in the criminal trial. On the other hand, in Delaware, because a criminal conviction is not required to bring a civil action, the plaintiff is in a much better position to recover damages from the defendant. The plaintiff need only prove a "knowing unauthorized access or alteration, etc.," by a preponderance of the evidence. Not only is the requisite intent of a lesser degree since it is merely knowing access and not intentional access, but the burden of proof is also of a lesser degree. In addition, if the plaintiff wins, he may recover attorney's fees. By not first requiring a violation of the criminal statute, Delaware and New Jersey have basically created a new cause of action for the plaintiff. Rather than sue under a common law tort theory such as trespass, which would be much more difficult, these states permit persons to show a trespass to their computers with a lesser degree of intent and a lesser degree of proof.

IV. TORT LIABILITY FOR COMPUTER VIRUSES

Once the creator of a computer virus has been convicted under either a state or federal criminal statute, statutes allowing civil remedies[122] provide the victim with an easier method of obtaining damages because the criminal proceeding usually will have already proven the case against the defendant. However, if the perpetrator has not been convicted, or if the statute does not provide for civil remedies, the victim may be unable to recover damages under the statute. Moreover, suing under a state or federal statute may present evidentiary problems,[123] as well as difficulty in establishing the requisite intent.

Nonetheless, victims of computer crimes are not limited to the civil remedies available under criminal statutes. In addition to statutory remedies, victims of computer viruses may rely on several tort theories to recover damages. In some cases, victims may use state criminal statutes by analogy under a negligence theory. In other cases, victims may bring civil actions under the common law theories of negligence, trespass to chattel, conversion, intentional interference with business relations, and products liability. This section will explore the various tort theories and their applicability to computer viruses.

A. USING CRIMINAL STATUTES BY ANALOGY IN CIVIL ACTIONS

In states where computer crime statutes do not specifically provide for civil actions, victims of computer viruses may be able to use criminal

122. *See supra* note 56.

123. Note, *Computer Crime and the Computer Fraud and Abuse Act of 1986*, 10 COMPUTER/L.J. 71, 83 (1990).

statutes by analogy in common law negligence actions. A common law negligence action generally requires that the plaintiff prove all the elements of negligence: duty, breach, cause in fact, proximate cause, and damages.[124] However, in using a criminal statute by analogy, the statute can establish the elements of duty and breach if the defendant violates the statute.[125] Violation of a statute could constitute conclusive evidence of negligence (negligence per se).[126] Generally, if specific provisions in the statute authorize the imposition of civil penalties,[127] then inquiring into the legislative intent is unnecessary.[128] Nonetheless, if the statute does authorize a civil action, then using the criminal statute by analogy is unnecessary in most cases because the plaintiff would probably prefer to sue under the statute. One situation where the plaintiff might want to pursue a negligence action based on a criminal statute is where the civil provision does not award sufficient damages to cover the actual damages incurred by the plaintiff. In that situation, the plaintiff can pursue an independent civil action based on the criminal statute by analogy or bring both causes of action in order to maximize recovery.[129]

In order for the criminal statute to apply, the legislature must have intended that the statute protect the class of persons that includes plaintiff and protect against the risk of the type of harm which has in fact occurred as a result of its violation.[130] The Minnesota statute governing destructive computer programs illustrates how a criminal statute will apply to negligence actions. Minnesota recently enacted the Computer Virus Act[131] which amends its current computer crime laws to cover the threat of computer viruses. The Act does not specifically provide for civil remedies. Many courts, however, are willing to find an "implied" legislative intent to provide a civil remedy within the statute.[132] This "implied intent" appears in a companion section regarding computer theft. A cross-reference under this particular section refers to civil liability for theft pursuant to section 332.51.[133] Although the legislature did not set forth a civil remedy in the amended sections, the

124. *See infra* notes 148-51 and accompanying text.

125. W. KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 36, at 229-30 (5th ed. 1984). [hereinafter PROSSER].

126. *Id.* § 36, at 220 n.2.

127. *See supra* note 56.

128. PROSSER, *supra* note 125, § 36, at 220.

129. Most states providing civil remedies under criminal statutes allow the aggrieved person to pursue any cause of action *in addition to* the civil action under the statute. *See supra* note 56.

130. PROSSER, *supra* note 125, § 36, at 224-25.

131. MINN. STAT. ANN. § 609.87.

132. *See supra* note 130 and accompanying text.

133. MINN. STAT. ANN. § 609.89.

fact that civil remedies are available for *computer theft* strengthens the argument that these remedies should be available for all *computer-related offenses.*

The first part of the negligence per se analysis focuses on the class of persons protected. Statutes that prohibit the destruction, deletion, access or alteration of any computer, computer system, or computer program intend to protect the owners, lessees, or operators of such computers.[134] Because owners, lessees or operators of such computers generally have a work-related, business, or financial interest in computers, computer-related offenses affect them the most. Thus, they constitute the class of protected plaintiffs in a computer virus case. Most plaintiffs will satisfy the first step in the negligence per se analysis because the computer offense statutes specify the type of offense, damage, and most importantly, the chattel to which they apply.[135]

Assuming the plaintiff is within the class of persons protected by the statute, the second step is to determine whether the statute protects against the risk of the type of harm that has occurred as a result of a violation of such statute. The Minnesota Act defines a destructive computer program as "a computer program that performs a destructive function or produces a destructive product. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program, disables the computer . . . , or destroys or alters computer programs or data."[136] This statute specifically addresses the harm that such a program can cause, notably the computer damage addressed in section 609.88. Subdivision (c) of this section makes the distribution of a destructive computer program "without authorization and with intent to *damage or destroy* any computer" a punishable offense.[137] Depending on the type of virus, the "harm" in a computer virus case may be the erasure or loss of valuable data, the malfunction of the computer or the entire computer system, and possibly, the complete destruction of a computer.[138] Minnesota's statute clearly protects the plaintiff against any damage or destruction done to a computer since it prohibits anyone from distributing a virus with the *intent to damage or destroy a computer.*[139]

---

134. "It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." CAL. PENAL CODE § 502(a).

135. *Id.*

136. MINN. STAT. ANN. § 609.87, subd. 12.

137. *Id.* § 609.88(c).

138. *See supra* notes 3-5.

139. MINN. STAT. ANN. § 609.88.

As long as the victim of a computer virus can establish that he belongs to the class of persons protected by the statute, and that the statute encompasses the type of harm that has occurred as a result of the statute's violation, he will conclusively establish duty and breach.[140] The plaintiff must then prove the defendant's negligence actually and legally caused his injuries. This burden may be especially difficult with computer viruses.[141] In addition, the plaintiff must also show that the defendant violated the statute to establish the defendant's negligence.[142] As discussed previously, this presents problems as to the perpetrator's "intent" to commit the crime.[143] In spite of the causation and "intent" difficulties that a plaintiff may encounter, using a criminal statute by analogy to establish negligence might be an effective method for the plaintiff to obtain damages in states that do not specifically provide civil remedies for computer-related offenses.

B. NEGLIGENCE

Under a common law claim for negligence, the plaintiff must prove the defendant had a legal duty to protect the plaintiff against an unreasonable risk of harm,[144] the defendant breached that duty,[145] the breach proximately caused the harm done to the plaintiff,[146] and the plaintiff did in fact suffer harm as a result of the breach.[147] Negligence may apply to a computer virus case in two ways. As discussed previously, the first method applies the elements of negligence using a criminal statute.

---

140. PROSSER, *supra* note 125, § 36, at 230. While a majority of jurisdictions hold that a plaintiff conclusively establishes negligence by demonstating that a defendant violated a criminal statute, some jurisdictions, such as California, hold that a violation creates merely a presumption of negligence. The four elements that a plaintiff must show for the presumption to apply are as follows: (1) a violation; (2) the violation was the proximate cause of the injury; (3) the injury is of the type the statute was designed to prevent; and (4) the plaintiff is a member of the class the statute was enacted to protect. "The presumption may be rebutted if the violator shows that he did what might reasonably be expected of a person of ordinary prudence, who desired to comply with the law . . . ." *Id.* at 230 n.9 (*citing* Byrne v. City & County of San Francisco, 170 Cal. Rptr. 302 (Ct. App. 1980)). Still other jurisdictions hold that a violation is "only evidence of negligence, or, prima facie evidence thereof." *Id.* at 230.

141. "Even if . . . negligence is proved, the actual cause of harm could be erroneous input, a hardware failure, a power failure, or an error of the system operator." 3 D. BENDER, COMPUTER LAW LITIGATION, § 11.03[2][c], at 11-14 (1991) (discussing general causation problems in a computer-related negligence action) [hereinafter BENDER].

142. *See supra* text accompanying note 125; *see also* PROSSER, *supra* note 125, § 36, at 229-30.

143. *See, e.g., supra* note 139 and accompanying text.

144. PROSSER, *supra* note 125, § 36, at 164-65. *See also* BENDER, *supra* note 141, at 11-14.

145. PROSSER, *supra* note 125, § 36, at 164-65.

146. *Id.*

147. *Id.*

The second method applies the elements of negligence to the dissemination of a computer virus using the standard of "ordinary care."[148]

In applying the second method to establish negligence, it may be helpful to analogize a computer virus to a biological virus.[149] "Just as a biological virus uses 'the biochemical mechanisms of a host cell to'[150] replicate, a computer virus produces new copies of itself by using other software."[151] Additionally, a biological virus may cause an infection that "remain[s] latent for long periods in an infected host before the appearance of clinical symptoms,"[152] just as a program infected by a computer virus does not usually execute the ultimate function of the virus immediately.[153]

Because of the similarity between a computer virus and a biological virus, cases dealing with sexually transmitted diseases prove helpful in analyzing a computer virus under a negligence theory. In *Jane Doe v. Richard Roe*,[154] the California Supreme Court relied on *Tarasoff v. Regents of the University of California*[155] to determine whether it should impose a duty on the defendant after transmitting herpes to the plaintiff.[156] The court relied on the basic principle expressed in California Civil Code section 1714 that everyone is responsible for "injury occasioned to another by his own want of ordinary care or skill."[157] The *Doe* court affirmed the judgment for the plaintiff, relying on several cases that have recognized a cause of action for the transmission of a sexual disease.[158]

In deciding whether to impose a duty when a defendant transmits a sexual disease, or when a defendant transmits a computer virus, courts will often look to a number of policy considerations.[159] In *Doe*, the

148. *Id.* at 209-10.

149. *See* Tramontana, *supra* note 4, at 254-55.

150. *Id.* at 255 n.11.

151. *Id.* at 254-55.

152. *Id.*

153. *Id.*

154. 267 Cal. Rptr. 564 (Ct. App. 1990).

155. 551 P.2d 334 (Cal. 1976).

156. *Doe*, 267 Cal. Rptr. at 566.

157. *Id.*; *see also Tarasoff*, 551 P.2d at 342.

158. *Doe*, 267 Cal. Rptr. at 567; *see* Mussivand v. David, 544 N.E.2d 265, 269-70 (Ohio 1989) ("Thus people suffering from genital herpes generally have a duty either to avoid sexual contact with uninfected persons or, at least to warn potential sex partners that they have herpes before sexual contact occurs.").

159. Policy considerations include the following:

> the foreseeability of the harm suffered, the degree of certainty the plaintiff suffered injury, the closeness of the connection between defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care, and the availability, cost and prevalence of insurance for the risk involved.

court recognized the state's strong interest in preventing the spread of a serious and incurable disease such as herpes.[160] In a computer virus case, for instance, a court will likely recognize a similar state interest in protecting computer users from the type of harm created by the spread of a virus. Once set in motion, a malignant computer virus, like a disease such as herpes, cannot be cured—it will either destroy every computer program it infects, which could mean thousands of programs, or it may self-destruct. The danger presented by computer viruses is that valuable computer data, as well as the computer hardware itself, could be permanently lost or destroyed, affecting thousands of computer owners and users.

Although computer virus cases can be analogized to cases finding a defendant negligent for transmitting a sexual disease, because computer viruses create purely economic harm, courts may impose stricter requirements on a plaintiff to prove the elements of breach and causation.[161] However, assuming that policy arguments will outweigh the causation problems,[162] the victim of a computer virus will likely have a strong case under an ordinary negligence theory.

C. INTENTIONAL TORTS

1. *Trespass to Chattel*

Several intentional torts may apply to computer virus cases. The first tort is common law trespass to chattel. Trespass to chattel includes any direct and immediate intentional interference with a chattel in the possession of another.[163] The plaintiff must show that the person intended to carry out the conduct that caused the harm and that the harm was of a kind the person knew or should have known would reasonably result as a consequence of his or her actions.[164] Assuming the plaintiff prevails, he may recover the cost of repair or the replacement value of the property.[165]

Tarasoff, 551 P.2d at 342.

160. *Doe*, 267 Cal. Rptr. at 567.

161. "The degree of foreseeability necessary to warrant the finding of a duty will . . . vary from case to case. For example, in cases where the burden of preventing future harm is great, a high degree of foreseeability may be required." *Id.* at 566-67.

162. *See supra* note 159.

163. PROSSER, *supra* note 125, § 36, at 85 ("Thus it is a trespass to damage goods or destroy them, to make an unpermitted use of them, or to move them from one place to another.").

164. Samuelson, *Can Hackers Be Sued for Damages Caused by Computer Viruses?*, 32 COMM. OF THE ACM 666, 668 (1989) (LEXIS, NEXIS library, Trade/Tech File) [hereinafter Samuelson].

165. Zaslow v. Kroenert, 176 P.2d 1, 7 (Cal. 1946).

In a computer virus case, the plaintiff must prove the defendant intentionally interfered with the plaintiff's possession of the computer. The plaintiff must show either that the interference destroyed or damaged the computer or its program or that the defendant made an unpermitted use of the computer or program.[166] Assuming the plaintiff can prove the requisite intent to cause the interference, he is entitled to recover actual damages.[167] In a computer virus case, such damages include the loss of computing time, the cost of system clean up, destroyed programs or data, and/or the cost of installing new security measures.[168]

2. *Conversion*

The second intentional tort that might apply to computer viruses is the tort of conversion. Conversion is the intentional exercise of dominion or control over another's chattel that substantially interferes with the other's right to control. As a result, the actor may be required to pay the other for the full value of the chattel involved.[169] In *National Surety Corp. v. Applied Systems, Inc.*,[170] a former employee converted certain computer programs belonging to his employer.[171] The defendant argued that since a computer program constitutes "intangible property," the conversion statute was inapplicable.[172] The court, however, held that the Alabama conversion statute applied to *all property*, tangible or intangible,[173] and that it applied not only to wrongful takings, but also to illegal assumption of ownership, illegal use or misuse, and wrongful detention.[174]

As *National Surety* suggests, a person may convert the goods of another in several ways. Among the more traditional methods of conversion, substantial "damage or alteration" to the property of another is the type that would most likely encompass the harm caused by a computer virus.[175] The crucial component of conversion is that the defend-

166. *See supra* note 163 and accompanying text.

167. *Zaslow*, 176 P.2d at 7.

168. Samuelson, *supra* note 164, at 666.

169. RESTATEMENT (SECOND) OF TORTS § 222A (1965).

170. 418 So. 2d 847, 849 (Ala. 1982) ("A computer program, in appropriate circumstances, can be the subject of conversion.").

171. *Id.* at 847.

172. *Id.*

173. *Id.* at 849-50.

174. *Id.* at 849.

175. PROSSER, *supra* note 125, § 36, at 100-01. Other types of conversion are the following: (1) wrongfully acquiring possession of the plaintiff's chattel; (2) removing plaintiff's chattel with an intent to assume control over the chattel, or deprive the plaintiff of it; (3) unauthorized transfer or disposal of possession of the chattel to one who is not entitled to it; (4) refusal to surrender possession, or, wrongful withholding of possession, of the chat-

ant's intentional interference actually and seriously disturb the owner's possession of the chattel.[176] In a computer virus case, where the virus actually erases a program owned by the victim, or causes damage to the computer system requiring a substantial amount of repair, the victim may maintain a conversion action to recover the full value of the property converted.[177] However, because the victim may recover only the "value of the property converted,"[178] the victim may recover only the value of the program erased or the value of the repairs. In each case, the amount of damages must be "substantial;"[179] and, in most computer virus cases, the damages may not be substantial enough to result in a conversion. Courts may interpret "substantial" to mean loss of the entire chattel, namely, the computer. In most computer virus cases, the programs within the computer system are lost or destroyed, but the computer hardware itself remains intact. However, due to the increasing number of viruses infiltrating the computer world, a court may very well determine that the *value of the programs* lost or destroyed is substantial enough to amount to a conversion.

3. *Intentional Interference with Business Relations*

The final intentional tort that might apply to computer viruses is intentional interference with business relations. This tort takes the form of either interference with contractual relations[180] or interference with prospective advantage.[181] A court may impose tort liability on a defendant who intentionally and improperly interferes with the plaintiff's rights under a contract with another person if the interference causes the plaintiff to lose a right under the contract or makes the contract rights more costly or less valuable.[182]

In order for this tort to apply, the plaintiff must meet two requirements. First, the plaintiff must demonstrate that the defendant intended to interfere with the plaintiff's contractual relations, at least in the sense that he acted with knowledge that interference would re-

---

tel to one who is entitled to it; and, (5) substantial use of the chattel, exceeding that which is permitted or authorized. *Id.* § 36, at 93-101.

176. "Where the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damage to the personal property, the owner has a cause of action for trespass . . . , and may recover only the actual damages suffered . . . ." Zaslow v. Kroenert, 176 P.2d 1, 7 (Cal. 1946).

177. PROSSER, *supra* note 125, § 36, at 106.

178. *Id.*

179. *Id.* § 36, at 101.

180. *Id.* § 36, at 978.

181. *Id.* § 36, at 1005.

182. RESTATEMENT (SECOND) OF TORTS § 766.

sult.[183] Second, the plaintiff must establish that the defendant acted for an improper purpose.[184] Clearly, if someone creates a computer virus and intentionally transmits the virus to computers the person knows are used for business purposes, and the virus erases programs containing business files or interferes with the system so that the business cannot operate properly, the victim may bring an action for intentional interference with contractual relations.

Even if no contract is involved, the victim may recover damages under intentional interference with prospective advantage.[185] For example, a hacker who infects a banking system with a virus might be responsible for the bank's loss of income or profits under a theory of interference with prospective advantage[186] even where no contracts are involved. Extending liability even further, the California Supreme Court[187] permitted liability based on negligence by balancing such factors as foreseeability, closeness of connection, and moral blame.[188] Apparently, when a computer virus interferes with business or economic dealings and the plaintiff can prove the defendant's intent to interfere,[189] an improper purpose, and when such interference resulted in a loss of profits or income, the plaintiff should be able to recover damages for the losses incurred.

An action based on intentional interference with business relations would give the plaintiff a more complete remedy then where the plaintiff sues under a criminal statute, but the civil remedies available do not include loss of profits. By bringing a second action under this theory, the plaintiff would be able to maximize his recovery, especially where the virus has destroyed valuable data on an existing contract, or proposed contract, with another entity. If the plaintiff lost business due to the destruction of the data, he should pursue an action based on inten-

183. *Id.*

184. "The defendant has been held liable if the reason underlying his interference is purely a malevolent one, and a desire to do harm to the plaintiff for its own sake." PROSSER, *supra* note 125, § 36, at 1009.

185. *Id.* § 36, at 1006.

186. Bequai, *Hackers Beware: Legal Sanctions Are on the Books*, 6 DIGITAL REV. 55, 56 (1989) (LEXIS, NEXIS library, Trade/Tech File).

187. J'aire Corp. v. Gregory, 598 P.2d 60 (Cal. 1979).

188. *Id.* at 63. *See* PROSSER, *supra* note 125, § 36, at 1008 n.35 ("The court would also consider the extent to which the transaction was 'intended' to affect the plaintiff," apparently requiring only a certainty that the plaintiff would be affected rather than an intent to harm him. Other factors the court would consider include the "certainty of harm and the policy of deterring future conduct.").

189. Under California law, a mere showing of negligence by balancing the factors discussed above would result in a favorable finding for the plaintiff. *See supra* note 188 and accompanying text.

tional interference with business relations in addition to actual damages.

D. PRODUCTS LIABILITY

Although several theories may apply in a products liability case,[190] this Comment deals solely with the theory of strict liability[191] as applied to cases where a software vendor sells a product containing a computer virus.[192]

Perhaps the most serious threat to computer users is to become the victim of a computer virus through a commercially-packaged software program, rather than through an electronic bulletin board.[193] Viruses found in commercial software are rare occurrences,[194] but they can lead to devastating results for the vendor as well as for the buyer.[195] In one instance, a perpetrator propagated a virus mainly by infecting a commercial product before release to the public.[196] In March 1988, Aldus Corporation, vendors of desk-top publishing software, inadvertently shipped hundreds of copies of a new software product containing a virus.[197] "Since over 100,000 users were infected, the release of this virus, and ensuing publicity, immeasurably damaged Aldus' reputation in the software market."[198]

The primary motivations for applying strict liability to products appear to implicate the computer industry:

---

190. Along with strict liability, negligence and breach of warranty may apply to products liability cases. *See* Note, *Software Vendors' Exposure to Products Liability for Computer Viruses*, 9 COMPUTER/L.J. 509 (1989).

191. Section 402A of the Restatement (Second) provides:

> (1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if
> (a) the seller is engaged in the business of selling such a product, and
> (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

RESTATEMENT (SECOND) OF TORTS § 402A.

192. Note, *supra* note 190.

193. Unlike commercial software, electronic bulletin boards threaten a user who has accepted the risk of a computer virus in exchange for free access to information. *See* Thornburg, *Computer Viruses Use Networks to Spread the Disease of Distrust*, COMPUTE!, July 1988, at 10.

194. Karon, *The Hype Behind Computer Viruses: Their Bark May be Worse than Their 'Byte,'* PC WEEK, May 31, 1988, at 49.

195. Kluth, *supra* note 30, at 301-02.

196. *Id.*

197. Note, *supra* note 4, at 259.

198. Kluth, *supra* note 30, at 301-02. *See also* Johnson, *Computer Virus Spreads to Commercial Software*, INFOWORLD, Mar. 21, 1988, at 85 (discussion of how virus infected software).

> First, the party in the best position to detect and eliminate defects should be responsible for damages inflicted by defective products. Second, liability should be placed upon the party best able to absorb and spread the risk or cost of injuries through insurance. Third, a remedy should not be prevented by burdensome requirements of proof since an injured person is not normally in a position to identify the cause of the defect. Fourth, due to modern marketing methods, consumers rely on the reputation of a manufacturer and no longer adhere to the doctrine of caveat emptor.[199]

These policy reasons for applying strict liability to products apply equally well to a situation where a software vendor sells a program containing a virus to a consumer. A consumer is not likely to recognize that a virus is causing problems with the software. Because the originator of the program possesses superior knowledge about the program, he or she is in a better position to diagnose the cause of the defect. Generally, the person in a better position to determine a product's defects should be held to a higher degree of care. Under the theory of strict liability, the seller is strictly liable for any product sold in a defective condition regardless of whether the seller was negligent or not.[200]

Although the "policy reasons for imposing strict liability may seem sensible, actually applying strict liability to software defects could prove extremely difficult."[201] In addition to the problems of application, even if the plaintiff can prove the requisite elements,[202] the vendor is generally only liable for physical harm to the consumer or to his property, not for economic loss.[203] Physical harm to property would encompass actual damage to the computer system or hardware, but it is questionable whether the data stored in the computer would constitute property within the definition of strict liability. The data or programs are probably intangible property, but if a court considers intangible property to fall within the definition of strict liability, then it could consider erasure or destruction of such data as "physical harm to property."[204]

However, the most difficult obstacle for a plaintiff to overcome in applying strict liability is proving that the defective condition is unreasonably dangerous; courts do not generally consider a virus-infected program "unreasonably dangerous."[205] The reluctancy to label programs "unreasonably dangerous" stems from the fact that the imposi-

---

199. Note, *Strict Products Liability and Computer Software: Caveat Vendor*, 4 COMPUTER/L.J. 373 (1983).

200. RESTATEMENT (SECOND) OF TORTS § 402A.

201. *See* Note, *supra* note 190, at 524.

202. RESTATEMENT (SECOND) OF TORTS § 402A.

203. Gemignani, *Product Liability and Software*, RUTGERS COMPUTER & TECH. L.J. 173, 197 (1981).

204. RESTATEMENT (SECOND) OF TORTS § 402A.

205. *Id.* at 525.

tion of strict liability may occur in a limited setting, such as where the defendant mass-markets the product and the application involves a potentially dangerous activity.[206] However, a few instances may arise where a virus-infected program would be highly dangerous. For example, programs used to monitor air traffic or control nuclear power plants, if infected by a computer virus, could easily be considered an unreasonably dangerous condition.[207] Although strict liability may have limited application in a computer virus situation, it could provide the plaintiff with an effective means of recovering damages caused by the virus.

V. PREVENTIVE MEASURES AND ALTERNATIVES TO CIVIL REMEDIES

Although recovering damages may be the most satisfying remedy, in many instances civil actions will be futile. Often, a typical computer vandal may have little money with which to pay a judgment.[208] In addition, bringing a civil action can be expensive and time consuming for the person affected by a virus. However, "the law does allow someone who has obtained a judgment against another person to renew the judgment periodically to await 'executing' it until the hacker has gotten a well-paying job or some other major asset which can be seized to satisfy the judgment."[209] If the victim of a computer virus does not choose to take civil action, either because a simple cost/benefit analysis reveals that the costs of a lawsuit far outweigh the amount of damages recoverable or because the perpetrator is "judgment-proof,"[210] several alternatives are still available.

A. SECURITY MEASURES

The availablity of civil remedies and criminal punishment for computer viruses has produced a tremendous increase in security measures.[211] Specialists agree that an increase in computer access security is a necessary step toward limiting the potential impact of virus programs

206. Note, *supra* note 190, at 526.

207. Gemignani, *supra* note 203, at 197.

208. Note, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 634 (1989).

209. Samuelson, *supra* note 164.

210. "Judgment-proof" refers to defendants who have little or no assets with which to secure a judgment against them. BLACK'S LAW DICTIONARY 845 (6th ed. 1990).

211. *See* R. BURGER, COMPUTER VIRUSES A HIGH-TECH DISEASE 81-91 (1988) (discussing various protection strategies that can be implemented by users to limit the potential impact of computer viruses) [hereinafter BURGER]. *See also* Marshall, *The Scourge of Computer Viruses*, 240 SCIENCE 134 (1988) (discussing many of the anti-virus programs that are currently available to users wanting to protect their software).

on computer systems.[212] However, security measures by themselves probably will not be an adequate safeguard against viruses because they create an inviting challenge to computer programmers.[213]

The recent publicity surrounding computer viruses has triggered a growth of computer vaccine programs.[214] Computer specialists suggest that vaccine programs be part of a comprehensive computer security plan[215] in order to provide the most effective means of preventing computer viruses from infiltrating computer systems. While no system can be totally secure, implementing tighter security measures can save businesses, governments, and consumers from more damaging losses.[216]

B. INSURANCE COVERAGE

One alternative to civil remedies is for computer users to obtain insurance coverage.[217] One author has suggested that "compulsory insurance coverage, such as that required by operators of motor vehicles[,] . . . may provide compensation for unanticipated losses."[218] Insurance can provide an additional means of protection against computer viruses and can minimize the amount of damages caused by a virus. Accompanied by tighter security measures, it can be an effective alternative to civil remedies or criminal punishment.

Perhaps the most effective coverage comes not from the victim's policy, but rather from the perpetrator's homeowner policy that covers all negligence claims. If the plaintiff brings a negligence suit against the creator of a computer virus,[219] he could recover monetary damages from the defendant's insurance company. In an unpublished opinion,[220] a Wisconsin appellate court held a defendant negligent for transmitting a sexual disease to the plaintiff[221] and found that the defendant's home-

---

212. BURGER, *supra* note 211, at 82.

213. McLellan, *Computer Systems Under Seige*, N.Y. TIMES, Jan. 31, 1988, at C1 (noting that increased security measures tempt programmers to develop better virus programs).

214. Marshall, *supra* note 210, at 134.

215. *See* Burgess, *'Virus' Attack Giving Boost to Computer Security Industry*, WASH. POST, Nov. 8, 1988, at D1.

216. Smith, *Who is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 110 (1985).

217. *Insurance May Cover Computer Virus Losses, Corroon & Black Corporation Specialist Says*, PR NEWSWIRE, May 24, 1989 (LEXIS, NEXIS Library, PR News File).

218. Branscomb, *supra* note 8, at 57.

219. *See supra* notes 144-48 and accompanying text.

220. Loveridge v. Chartier, No. 88-2107, 1989 Wisc. App. LEXIS 1168 (Wis. Ct. App. Dec. 13, 1989).

221. *See supra* notes 154-59 for discussion of computer viruses analogized to cases involving sexually transmitted diseases.

owner policy covered such action.[222] However, because insurance coverage usually extends only to negligent acts by the insured and not to intentional torts,[223] homeowner's policies would only be effective in negligence actions. Since most computer viruses are considered to be intentional acts, a computer virus victim may have difficulty obtaining damages from the defendant's insurance company.

VI. CONCLUSION

Criminal statutes designed to punish those who create computer viruses are the most effective means to deter hackers. However, these statutes give victims of viruses little satisfaction when they are left to pay the bills for cleanup costs, repairs, and tighter security programs. Civil remedies within criminal statutes give the victim an avenue to pursue an action against the perpetrator for damages as well as allow the perpetrator to receive the punishment he deserves. In the absence of these provisions, the victim may rely on criminal statutes by analogy along with common law claims such as negligence, intentional torts, and products liability to recover damages.

Where, however, the costs of bringing a civil action exceed the amount of damages, or the perpetrator is judgment-proof, the victim might want to avoid a civil action and rely on tighter security measures, anti-viral programs, and insurance coverage to prevent viruses from causing damage in the future. While this Comment explores the civil remedies available to the victims of computer viruses, it is clear that a criminal conviction is the most effective deterrent to prevent hackers from ever creating such malevolent programs. Deterrence is the most preferable remedy, but civil remedies provide the best alternative for making hackers "pay" for their transgressions.

Susan C. Lyman

222. *Loveridge*, No. 88-2107, 1989 Wisc. App. LEXIS 1168, at *1.
223. *Id.* at *2.