Richmond Journal of Law and Technology

Volume 8 | Issue 3 Article 5

2002

The Legislative Response to the Evolution of Computer Viruses

Mark R. Colombell
University of Richmond

Recommended Citation

Mark R. Colombell, *The Legislative Response to the Evolution of Computer Viruses*, 8 Rich. J.L. & Tech 18 (2002).
Available at: http://scholarship.richmond.edu/jolt/vol8/iss3/5

Volume VIII, Issue 3,

Spring 2002

The Legislative Response to the Evolution of Computer Viruses

by: Mark R. Colombell[*]

Cite As: Mark R. Colombell, *The Legislative Response to the Evolution of Computer Viruses*, 8 RICH. J.L. & TECH. 18 (Spring 2002) *at* http://www.jolt.richmond.edu/v8i3/article18.html.

TABLE OF CONTENTS

I. INTRODUCTION

{1}On July 19, 2001, and again on July 31, 2001, the United States Government was attacked by a worm. The Code Red worm, a malevolent computer program, spread across the Internet impacting thousands of computers globally. The initial target of the Code Red worm was the White House website. Just days after the terrorist attacks in New York, Washington D.C., and Pennsylvania on September 11, the Nimda virus was unleashed on the Internet. By consuming up to ten percent of the Internet's capacity, Nimda quickly received the distinction as the worst computer infestation to date.[1]

{2}The impact of the Nimda virus and the Code Red worm are just two examples of how people’s social and professional lives are dependent on computers. Access to the Internet permits individuals to share files from work, share jokes with friends, or e-mail family members. With the portability of computers and the introduction of wireless Internet access, computers and the Internet will play an even larger role in our day-to-day lives. Directly proportional to this increase in computer usage and Internet access is the increase of computer abuse and fraud. As an individual becomes more dependent on computers, the likelihood and incidence that the individual will be a victim of a computer crime greatly increases.

{3}A problem facing state, federal, and international governments is the need to contain the growth of "computer virus" crime. The severity and impact of computer virus crimes range from vandalism to terrorism.[2] Computer virus crime involves computer programmers intentionally destroying the host computer or its data with their programs. The goal of federal and state legislation is to provide prosecutors with tools and leverage enough to pursue criminal sanctions against those who commit computer virus crimes and to provide victims with recourse through civil remedies.

{4}A computer virus is defined as a "program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes."[3] Computer viruses, which are man-made, replicate themselves like cancerous cells and then infect and possibly disable a computer or an entire network. Although computer code is often written by people with advanced degrees in Computer Science, a simple virus[4] that can continually replicate itself is relatively easy to produce. Additionally, with the increased popularity of collecting computer viruses as a hobby, dangerous programs are easily attainable and distributable. Because computers play a much larger role in people's daily lives, the possibility that a virus will impact the workplace or the home is greatly increased.

{5}This comment explores the evolution and development of computer viruses, provides background on the genesis of computer viruses, and discusses the three most common forms of malevolent computer viruses. Secondly, this comment presents a time line of federal legislation aimed at curtailing the spread of computer viruses. Analyzing federal, state, and international legislation spanning the past fifteen years reveals the reasons why prosecutors are handcuffed in pursuing criminal penalties and why victims are limited in their ability to obtain civil sanctions. Additionally, this comment examines the accomplishments and shortcomings of federal computer virus legislation. Finally, this comment highlights particular state laws that attempt to fill the holes left by federal legislation, briefly addresses the concerns and focuses of international lawmakers, and addresses civil remedies for the victims of computer viruses.

II. THE EVOLUTION AND DEVELOPMENT OF COMPUTER VIRUSES

A. The First Self-Replicatng Program

{6}Seventeen years ago, in Rochester, New York, Xerox Corporation developed a program which continually self-replicated.[5] This self-cloning program, which was tested under controlled conditions, represented the first computer virus. Without realizing the possible negative implications, Xerox continually tested the computer virus over the span of a decade to evaluate the efficiency of computers serving troubleshooting functions.[6] Ten years after the invention of the first computer virus, the possible consequences of this emerging technology became evident, and Congress took notice.[7]

B. The Analogy of Computer Viruses to Human Viruses

{7}Computer virus programs penetrate personal computers and networks in a number of ways. Most commonly, computer viruses disguise themselves as harmless files that a computer does not recognize as being harmful. Much like a virus invading the human immune system, these destructive programs are extremely small, hard to locate, and dangerous.[8] When a virus infects the human body, the virus disguises its shape and form to resemble a human cell. The human body's defense system does not recognize the virus as foreign, and the virus is not attacked. The virus then overpowers other human cells, gradually multiplying and spreading, until the body recognizes the foreign invader and develops antibodies to combat the virus.[9]

{8}A computer virus works in the same manner. A computer virus cannot operate without a host computer system to infect. Viruses are written by programmers with the intention of executing certain functions by amending the original computer program with its own instructions.[10] Since a computer virus program is usually disguised as a harmless program, a computer is not able to distinguish between the instructions of the main program and those of the dangerous virus. Ultimately, a host computer is unable to detect a virus because of "hiding" functions viruses use to disguise themselves.[11]

{9}Just like a virus spreading throughout the human body, a computer virus attaches itself to other programs, clones itself, and damages the host system by taking up all available memory. Once a virus enters a computer, the program seeks to continually infect its host. When a virus is exposed to a new computer disk, the virus first checks the disk for an existing copy of itself. Virus programmers purposely install this "check" function to prevent tracking of the virus. If a disk check returns a negative result, the virus clones itself onto the uninfected disk. When given the chance, the virus will spread to new computers and repeat the same process.[12]

C. The Classification of Computer Viruses

{10}Like viruses in the human body, computer viruses are classified as either benign or malevolent. Viruses that cause the most damage are malevolent. Malevolent viruses are programmed to damage a computer.[13] In contrast, a benign virus is not specifically programmed to destroy a computer. Often, benign viruses are distributed to simply harass or interrupt the use and enjoyment of a computer. Benign viruses also can be harmful to a computer or network. Benign viruses can cause problems by consuming the computer's resources.[14] Because of the likelihood that they will inflict greater harm, legislators have shown more concern for the prevention and containment of malevolent viruses. Malevolent viruses can infect a number of different portions of the computer's operating and file systems.[15]

{11}Types of viruses that target areas within the operating or file systems include system sector viruses,[16] file viruses,[17] macro viruses,[18] companion viruses,[19] cluster viruses,[20] batch file viruses,[21] source code viruses[22] and Visual Basic worms.[23] The three most common malevolent viruses are worms, Trojan horses and logic bombs.[24]

D. Worms, Trojan Horses and Logic Bombs

{12}A worm program gets its designation from the way it slithers in and out of a computer network.[25] Like most computer viruses, a worm program is only dangerous when designed to perform some particular function.[26] Unfortunately, when a worm program is written to perform a negative function, the program "move[s] through a network and disable[s] computers by freezing keyboards and screens, filling memory, or slowing down computers."[27]

{13}Perhaps the most famous example of a worm is the virus released by Robert Morris Jr. in November 1988.[28] The worm program designed by Mr. Morris might be the most destructive computer virus on record.[29] Mr. Morris released a devastating worm program into a network of a branch of the United States Defense Department.[30] Morris, an experienced programmer, took specific measures to ensure that his program was not easily traceable.[31] By gaining access to the government network through a design flaw in the e-mail system,[32] the worm spread through idle computers and disabled more than 6,000. Morris was caught because he underestimated the number of times a computer would be asked if it had been infected, and enough copying occurred to permit tracing.[33] Morris was indicted and found guilty under the Computer Fraud and Abuse Act.[34]

{14}Recently, the United States Government was once again the target of a worm attack. Impacting more than 250,000 computers over a two-week period in July of 2001,[35] the "Code Red" worm continues to have a snowball effect by operating on a monthly cycle.[36] This worm does not harm individual computers by wiping out files, but rather, the Code Red virus takes control of the computers it infects and uses them to generate massive Internet traffic.[37]

{15}Disguised as a useful program, a Trojan horse virus is the most common malevolent program.[38] A computer or network will accept a Trojan horse virus because the program is read and recognized as beneficial to the system. The malevolent program is masked within the host program and seeks to perform a designated task constructed and ordered by the programmer.[39] The possible tasks a Trojan horse can perform are limitless.[40]

{16}A logic bomb is the simplest, yet possibly the most dangerous, of the malevolent computer viruses.[41] A programmer designs a logic bomb to detonate according to a predetermined event.[42] "Just like a real bomb, a logic bomb will lie dormant until triggered by some event."[43] Programmers can make almost any event a trigger. A logic bomb can be triggered by "a specific date, the number of times executed, a random number, or even a specific event such as deletion of an employee's payroll record."[44] The possible consequences when a logic bomb is triggered are countless. Logic bombs have been programmed to change random bytes of data on a disk or completely wipe out an entire hard drive.[45] Programmers often opt for the more stealthy attack of changing random data. Programmers prefer this more sinister attack "since it generally causes substantial damage before anyone notices that something is wrong."[46] Like most other forms of computer viruses, it is difficult to prevent a well-written logic bomb from doing damage.[47] Logic bombs received heightened attention with the Y2K scare several years ago. Thousands of skillful programmers gained intimate access to government, private sector, and individual computers to perform Y2K modifications. Despite the government and most companies taking strong precautions against sabotage, Y2K provided rogue programmers with the opportunity to insert logic bombs and traps producing substantial damage.[48]

E. The Evolution of the Computer Virus

{17}In 1995, a new type of virus surfaced which did not require the infected program to actually run on the host computer. With the increased use of Microsoft Office in the mid-1990s, a Word Concept Macro virus emerged that infected documents created by version 10.0 of Microsoft Word.[49] Because so many business and homes were dependent on Microsoft Word for their word processing needs, the virus quickly spread internationally through individuals sharing files via e-mail. This new type of virus poses a serious threat to individuals who use and share word processing files.[50]

{18}Virus authors, much like Dr. Frankenstein, are beginning to piece together and combine new viruses by relying on the strengths of previous virus code. The Nimda virus, which is part virus and part worm, is an example of this new "hybrid bug."[51] By combining the most damaging features of its predecessors,[52] Nimda epitomizes the evolving nature and creativity of virus authors.

III. LEGISLATION ADDRESSING COMPUTER VIRUSES

A. Common Law Approaches to Computer Crime

{19}Prior to legislation passed in 1984,[53] courts relied on common law principles to prosecute computer crimes. Courts resorted to drawing analogies between computer crimes and ordinary crimes, then applied traditional common law principles. Prosecutors found it quite difficult to relate such a highly technical crime, such as distributing a computer virus, with simple common law principles such as trespass.[54] As computers became more accessible to the public, both courts and legislators soon realized that legislation was needed to resolve the dispute.

B. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

{20}Ironically, in 1984,[55] after heavy lobbying from the general public and computer companies, Congress passed the first federal computer crime statute.[56] The Counterfeit Access Device and Computer Fraud and Abuse Act[57] lacked clear definitions of applicable computer terms and failed to provide clear jurisdictional boundaries for the courts. Computer crime legislation remained ambiguous until the Computer Fraud and Abuse Act of 1986 was passed two years later.

C. The Computer Fraud and Abuse Act of 1986

{21}In response to growing concern over the dangers of computer crime, Congress passed the Computer Fraud and Abuse Act of 1986.[58] The passing of this legislation marked the government's first effective step in the fight against computer crime. The law specified that "unauthorized access to a government computer" was a felony, and "trespass into a federal government computer" was a misdemeanor.[59] The criminal trial of Robert Morris produced one of the first landmark indictments and convictions under this Act.[60]

{22}Prosecution under the 1986 Act proved difficult because the Act prescribed too narrow a standard of culpability. The 1986 Act set forth a standard of "knowing" or "intentional actions" for six enumerated acts.[61] The six enumerated offenses are: (1) knowing unauthorized access to obtain information that is restricted for national security by Executive Order;[62] (2) intentional unauthorized access to information from a financial institution or consumer reporting agency;[63](3) intentional unauthorized access that interferes with government operation of government computers;[64] (4) knowing unauthorized access to a government computer with the intent to defraud which results in obtaining anything of value other than the use of the computer;[65] (5) intentional unauthorized access to a federal interest computer that results in alteration, damage, or destruction of information in the computer or prevents authorized use of the computer or information;[66] and (6) knowingly trafficking passwords or similar information with the intent to defraud where the trafficking affects interstate or foreign commerce, or a federal interest computer.[67]

{23}Under the Act's standard of culpability, the programmer must "knowingly" or "intentionally" cause a particular act. Usually, a programmer spreading a computer virus does not know the identity of his individual victims.[68] A metaphor can be drawn between a programmer introducing a virus into a computer system and an individual letting a wolf into a chicken coup and shutting the door. Although the perpetrator does not know specifically which chickens will die, he does know that the wolf will cause substantial damage to as many chickens as possible. During the spread of a computer virus, a programmer has almost no control over how fast the virus spreads, how many computers it infects, or the amount of damage it causes.[69] The Act should have "cast a wider net" by prescribing a much broader *mens rea*. Unfortunately, imposing a lesser standard of culpability such as "recklessly" or "negligently" could implicate the countless innocent users who unintentionally spread the virus.

{24}Another problem with the 1986 Act was its failure to provide for broad interstate jurisdiction. By narrowly tailoring the Act to address only unauthorized access to federal interest computers and the interstate trafficking of passwords, the Act failed to provide a basis for prosecuting programmers when the virus traveled from state to state.[70] Failure to address this concern created a loophole in the Act for programmers who inserted viruses that eventually crossed state lines via e-mail.[71] Without broad federal jurisdiction, computer criminals often evaded state computer crime statutes that were unable to provide for personal jurisdiction over programmers located outside of the state or the country.

{25}Although the Act represented a substantial step forward in the relatively new realm of cyberspace, the ambiguity and the poor foresight in addressing civil remedies made it difficult for attorneys and judges to apply the law. Because many legislators were unfamiliar with the technical language of computers, the Act failed to provide clear and concise definitions of key terms. The ambiguity in key term definitions resulted in attorneys and judges arguing over the legislative intent of the Act, compounding the ineffectiveness of the law.[72] One of the most significant drawbacks of the 1986 Act was its failure to address civil remedies for property damage caused by a computer virus. Due to this void in civil remedies, it is likely that many computer viruses and crimes went unreported.[73]

D. Proposed Amendments to the 1986 Act

{26} The Computer Virus Eradication Act was first introduced in the House of Representatives as a reaction to several computer virus scares in the mid-1980s. The proposed bill was not reported out of the House Judiciary Committee.[74]

{27}One year later, Congressman Herger introduced H.R. 55, a proposed amendment[75] to the original Computer Fraud and Abuse Act of 1986. Realizing the shortcomings of the 1986 Act,[76] Congressman Herger set a goal of levying harsher penalties on persons who use viruses to interfere with computer operations. In much clearer language, the proposed amendment provided:

> Whoever knowingly inserts into a program for a computer, or a computer itself, information or commands, knowing or having reason to believe that such information or commands may cause loss, expense, or risk to health or welfare to (i) users of such computer or a computer on which such a program is run, or to persons who rely on information processes on such computer; or (ii) to users of any other computer or to persons who rely on information processed on any other computer.[77]

In order to increase the likelihood of computer crime prosecution, the proposed amendment recommended three additions to the original Act. First, since the government was more familiar with computer viruses, the proposed amendment provided clearer and more concise language describing virus programming activity. Secondly, the proposed amendment clearly defined a penalty for creating or spreading a computer virus. Finally, H.R. 55 established civil remedies for those impacted by computer viruses. The proposed act provided that the court could award attorneys' fees and other litigation fees in addition to any relief for property damage that the court deems appropriate.[78]

{28}With little case law on the effectiveness of the 1986 Act, Congress elected to delay passage of the amendment. The amendment would have made it much easier to prosecute cyber-terrorism.[79] By providing a clearer and more effective standard of culpability, the amendment called for federal prosecution of criminals who "willfully or maliciously tamper with a computer's software or hardware."[80] The proposed amendment could have armed judges with more flexible sentencing alternatives for computer crime offenders.

E. The National Information Infrasturcture Protection Act (NIIPA)

{29}In 1996, the most recent proposed amendment to the 1986 Act, the National Information Infrastructure Protection Act, was introduced and passed in Congress. Although the statutory construction of the bill is clearer and more aggressive than past amendments, the legislation still has not produced many convictions of programmers using computer viruses over the past three years. The newest legislative addition to the war on computer crime, "which previously only covered crimes involving computers in more than one state, now covers any computer with Internet access, even if all the computers involved in the crime are located within one state."[81]

{30}The most relevant portion of the new amendment is NIIPA section 1030(a)(5). Section 1030(a)(5)(A)(i) makes it a crime to "knowingly cause the transmission of a program, code, or command with the intent to cause damage."[82] Sections 1030(a)(5)(A)(ii) and (iii) criminalize the intentional accessing of a computer in excess of one's authority, and causing damage as a result of that conduct, regardless of intent.[83] As a result of lessening the *mens rea* for these computer crimes, individuals who transmit malevolent software, including viruses, are responsible even if the transmission was not intentional, but only reckless or negligent.[84] This most recent amendment has eliminated some of the loopholes left by previous legislation.[85]

F. The Legislative Reaction to Computer Viruses in the Wake of the Septembre 11th Attacks on the United States.

{31}Computer crime legislation, similar to environmental law, is generally reactionary. It usually takes a tragedy or emergency to trigger a legislative response. Since the September 11th attacks, the National Security Agency and other federal government affiliates have been frantically working to address the legislative gaps which have weakened our informational security.[86] The Anti-Terrorism Act of 2001, which allows for the "easier prosecution and sentencing of computer hackers and web site vandals" could serve as the necessary reactionary step to address our informational security issues.[87]

{32}Several civil liberties groups have expressed concern about the overarching effects of new legislation that may "lump small-time hackers together with murderous terrorists."[88] Although this is a possibility, many believe that the increase in computer viruses and the terrorist attacks could be linked. It is well documented that the attacks on the World Trade Center and the Pentagon were symbolic attacks on the American economy and the United States military.[89] Virus attacks have impacted the United States both psychologically and economically, much like the terrorist attacks.[90] Experts point to the methodical nature and to the level of sophistication of the computer attacks which have exposed security weaknesses in private industry and the government.[91] Many groups, such as the Muslim Hackers' Club, have grabbed the attention of authorities following the computer virus outbreak seen in the past six months.[92] The Muslim Hackers' Club operates a website that provides users with hacking tips, "free software that enables unbreakable encryption as well as anonymous e-mailing and instructions on how to use viruses."[93]

G. Approaches of the States in Combating Computer Viruses

{33}As of 1997, forty-nine of the fifty states had passed computer crime legislation.[94] Recognizing a flaw in the federal approach to prosecuting these criminals, many states have designed stricter laws with harsher penalties for cyber-terrorists.[95] In order to more effectively prosecute cyber-criminals, current state laws provide clearer and more concise definitions, more flexibility in sentencing alternatives, and harsher penalties than their federal counterpart.

{34}For instance, no federal government legislation provides an actual definition of a computer virus. A recent bill passed by the state of Maine defines a computer virus as “any instruction, information, data or program that degrades the performance of a computer resource; disables, damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer program is executed.”[96] By providing a solid definition of a computer virus, Maine has provided its courts with a clear understanding of what constitutes a virus-related computer crime.

{35}The state of Oklahoma provides harsher penalties than the federal government for the spreading of a computer virus. Under one Oklahoma statute, a programmer, who spreads a virus, may be fined up to $100,000 and may receive a maximum prison sentence of ten years.[97] This punishment available to Oklahoma courts is more flexible than that outlined in the 1997 Act passed by Congress that recommends a fine and a maximum five-year prison sentence. Maine and Oklahoma are just two examples of state legislatures who have attempted to amend the shortcomings of federal legislation.

{36}In response to the many different statutes in the United States under which cyber-criminals can be charged, the federal government has attempted to tailor legislation specifically aimed at computer virus deterrence. As a result, the United States has treated cyber-crime as a distinct federal offense since 1984. By not providing enough deference to the states in their endeavor to enforce and prosecute computer virus crimes, the federal government has limited the resources at its disposal to prevent and deter computer crime.

H. Approaches of International Legislature in Combating Computer Viruses

{37}Countries throughout the world agree that a "coordinated international effort to fight computer crimes" is required.[98] With the increasing speed of processors and Internet connections, worldwide computer systems can be accessed from almost anywhere. This leaves every computer system vulnerable to a virus attack from anywhere in the world. There are four main goals that international lawmakers are emphasizing: (1) protection of privacy; (2) prosecution of economic crimes; (3) protection of intellectual property; and (4) procedural provisions to aid in the prosecution of computer crimes.[99] In order to accomplish these goals, international lawmakers must overcome the following obstacles.

1. Enforcement

{38}Although the international community has recognized the threat that computer viruses pose, it is apparent that "domestic laws are inadequate when attempting to prosecute virus authors located on foreign soil."[100] Just as state and federal prosecutors in the United States have had difficulty enforcing computer virus crime laws, so has the international community.

{39}One problem faced by every government is the inability to quickly apprehend a perpetrator.[101] The reason for the delay in catching the computer virus author is the lack of a coordinated international effort to bring perpetrators to justice. Usually countries are unable to respond in a timely fashion, producing great delays for an expedited investigation.[102] There are several reasons for the delayed response between countries. First, prosecution and enforcement of computer crime is not a top priority for most countries. Countries that are enduring civil unrest or political strife have more important concerns than dedicating valuable resources to catch a computer hacker. The second reason that international hunts for computer virus authors are so slow is the red tape of international relations.[103] Often, the complex nature of the legal process or poor relations between countries results in a loss of momentum in investigations.[104] The international community must work with the United States to draft procedural provisions to aid in the prosecution of computer crimes.

{40}A collaborated effort to catch a cyber-criminal involving all levels of the government and foreign countries is not only possible, but has already been accomplished. An example of such a collaborated effort was the pursuit and prosecution of David Smith, the author of the Melissa virus that spread across the Internet in March of 1999.[105] The Melissa virus was the fastest spreading virus the United States had ever seen and caused eighty billion dollars in damages.[106] The Melissa virus spread globally across e-mail, and after just two days, the impact of the virus caused servers at companies such as Microsoft and Intel to shut down.[107] "David Smith was caught through the combined efforts of private companies, individual Internet users in Sweden and the United States, America Online, and federal and state law enforcement."[108] Smith pled guilty to both the state and federal criminal charges brought against him. However, Smith's capture and prosecution were more the result of poor decisions made on his part than of the cooperation of these entities.[109] Smith authored and released the virus in the United States. Smith also remained in the United States after the release and spread of the virus. If Smith authored the virus in a country without adequate computer crime legislation or fled to another country after the release, he most likely would not have been caught.[110]

2. Extradition

{41}The method of extradition for computer virus authors is one of the most troublesome obstacles facing international lawmakers. Extradition and the laws governing computer crimes are not keeping pace with the changing faces of cyber-crime and cyber-criminals. Another problem is that certain aspects of computer crime legislation are not compatible with extradition.[111] Successful extradition relies a great deal on good will between cooperating countries; however, the lack of conformity in international treaties aimed at curtailing computer crime has resulted in poor communication and cooperation between countries.

{42}For example, extradition arrangements drafted by the United States are more formal in nature than those of most other countries. The arrangements struck by the United States usually require reciprocity, a treaty and double criminality. Reciprocity is based on the fundamental principal that "if I scratch your back, you will scratch mine." In others words, "if one nation honors another country's request for extradition, the requesting nation will do likewise when the situation is reversed."[112] But no matter how good the relations are between a foreign country and the United States, the United States will deny extradition if no treaty has been entered into. Another requirement of the United States in extradition agreements is double criminality – "the offense charged [must] be considered criminal in both the requesting and requested jurisdictions."[113] The double criminality provision required by the United States creates an easy loophole for computer virus authors. Many international countries do not even have legislation addressing computer virus crime. Another problem is that the severity of punishment and the regulation of computers and the Internet vary drastically from country to country.

{43}A collaborative effort between countries is required to bring cyber-criminals to justice. The international complications for prosecuting and punishing the spread of computer viruses must be remedied. For too long, countries have relied on their own independent legislation and investigation to catch these cyber-criminals. A possible solution to this problem is for the United States to loosen the requirements for extradition of cyber-criminals.

IV. CIVIL REMEDIES

{44}The first question the legislatures and courts must address regarding civil liability for computer virus damages is whether computer information should be considered legally protected property. In order to resolve liability issues, conformity must be established which recognizes the property value of computer information. Cases such as *CompuServe, Inc. v. Cyber Promotions, Inc.*[114] and *Thrifty-Tel, Inc. v. Bezenek*[115] reflect the trend of the courts and legislatures towards recognition of damage for the loss of computer information. Traditionally, the victims of computer crimes have sought relief in contract law,[116] not tort law, because of the economic loss rule.[117] However, courts are recognizing the fundamental unfairness of the economic loss rule as applied to computer crimes.[118]

A. Is Tort Law the Answer?

{45}Recovering civil damages through tort law has resulted in new problems that the courts must address. Courts have been slow to recognize computer information as legally protected property. Other problems raised by civil litigation in tort law for computer virus damage are personal jurisdictional boundaries and causation.[119] One possible solution to the civil questions raised by computer virus damage is that computer users assume the risk of computer virus infection by doing business electronically. However, this is not an adequate solution to a problem that can cause wide scale economic damage. The proper remedy can be found in negligence.

1. Parties to the Action

{46}In jurisdictions that provide for civil remedies, victims of computer virus who have sustained damage to their legally protected property can maintain a civil tort action and bring suit under the appropriate criminal statute.[120] However, victims will be out of luck in jurisdictions where computer data is not considered property. In these jurisdictions, any damages caused by a virus will be considered unrecoverable economic losses.

{47}However, just because a victim can bring suit for damages does not mean the victim will recover anything. One problem facing a victim is pinpointing the culprit. Victims will not want to pursue civil damages against an individual computer virus author for several reasons. First, an individual computer virus author is hard to catch. Secondly, even if the author is caught, it is unlikely that the author has "deep enough pockets" to make it worth the time and effort to attempt a damages recovery through the court system. Therefore, potential plaintiffs must look to pin liability elsewhere. The most likely candidates for defendants are the employers[121] of the tortfeasors who distribute the virus.[122] Yet, these companies will only be held liable for the negligent acts of their employees done within the scope of employment.[123]

2. Victims should have a remedy in Negligence.

{49}In order for a victim of a computer virus to recover in negligence, the plaintiff must prove all of the following elements: (a) a duty on defendant to use reasonable care; (b) a breach of that duty; (c) a reasonably close causal connection between defendant's conduct and the resulting injury, and; (d) actual loss or damage to a protected interest.[124]

a. The Duty of Reasonable Care.

{50}In order to recover, the victim must prove that the defendant corporation has a legal duty to the plaintiff to exercise reasonable care in maintaining adequate computer network security.[125] The corporation must have owed the plaintiff a duty to protect the victim from an unreasonable risk of harm that could result from the spread of a virus. The risk reasonably perceived determines the scope of "the duty owed and limits that duty to foreseeable plaintiffs."[126] Therefore, the victim of the computer crime must prove that the risk was foreseeable and that he could have been harmed by the introduction of a computer virus.

b. Breach of Duty.

{51}The second element of a negligence claim for damages inflicted by a computer virus requires the plaintiff to show that the corporation breached its duty to exercise reasonable care owed to the plaintiff.[127] A corporation can breach its duty owed to a plaintiff in a number of different ways. These breaches include the failure to recognize defects in its computer network security, the failure to correct defects, or the failure to warn of the defects.[128] Another way a plaintiff can show that a corporation breached its duty owed is to prove a "failure to train and supervise employees on adequate security procedures or failure to utilize reasonable means to secure the computer network from unauthorized use."[129]

c. Proximate Cause

{52}Thirdly, in order to successfully bring a negligence claim, the plaintiff must demonstrate proximate cause. To satisfy this element, the plaintiff must prove that the defendant's act or omission was the actual cause or cause-in-fact of the injury and that the plaintiff's injuries were the foreseeable consequence of the risk created by the defendant's act or omission.[130] If the plaintiff satisfies both of these prongs, the plaintiff has submitted a prima facie case of proximate cause.

d. Damages

{53} As mentioned earlier, courts have been reluctant to allow recovery for computer crimes based on negligence when plaintiff's loss was purely economical. Therefore, many plaintiffs who brought suit failed to prove legally cognizable damages, the fourth prong for a prima facie case of negligence. However, the modern trend of the courts to disregard the economic loss rule has made it easier for potential plaintiffs to prove damages and injury-in-fact.

V. CONCLUSION

{54} The origin of the computer virus spans back almost seventeen years. Over these years, programmers have developed means to make viruses more destructive and more stealthy. Computer viruses have evolved. Whether programmers rely on the three most common forms of malevolent viruses, the worm, the Trojan horse, and the logic bomb, or are developing new forms of viruses, it is apparent that the technological world will always remain one step ahead of the legislatures and the courts.

{55} Individuals and companies rightfully perceive computer viruses as a definite threat to personal property. With the increase in mobility and speed of computers, more and more people will be accessing the Internet and information that may leave them susceptible to cyber-terrorism. The threat of computer viruses has given rise to a large software industry aimed at preventing and disabling computer viruses.[131] Ironically, the anti-virus software companies seeking to curtail the spread of computer viruses may now be held liable for damages caused by the actions of another. Additionally, the more experience a person has with a computer and the Internet, the more knowledgeable she becomes in recognizing and avoiding potentially dangerous situations online. However, even the most experienced computer users cannot escape the wrath of a well-programmed computer virus. State, national, and international legislatures must address the problems of computer virus victims who feel they have no recourse in combating programmers who cause thousands of dollars in damage with a click of a mouse. Although recent legislation has provided a means for victims to collect damages, the legislation still fails to give full satisfaction to victims and does not provide harsh enough sanctions for the programmers causing these damages.

{56} The legislatures have taken strides in recognizing and addressing the severity of the problem. Several efforts have been made by both state and national legislatures to evolve with technology. However, the lack of criminal prosecution and civil liability for these programmers directly reflects the ineffectiveness of these laws. The challenge and excitement most programmers seek in spreading a virus is to wreak their havoc without getting caught. Programmers go to great lengths to develop viruses that are untraceable. Because virus spreaders are so tough to catch, the government should make examples of those programmers who do slip up. However, the standards of culpability for most computer crime statutes are still too stringent. By requiring the prosecuting attorney to show that the programmer intentionally or knowingly caused a certain amount of damage may be too strict to be effective.

{57} In order to provide prosecutors with enough firepower to combat cyber-terrorists, the standard of culpability for spreading a computer virus might have to be lessened to “recklessly.”[132] State legislatures have demonstrated enough initiative to draft tougher computer crime laws. Many states have recognized the deficiency of the federal legislation addressing computer crime and have passed their own legislation to deal with cyber-criminals. However, even with tougher state laws, states are still faced with problems such as establishing personal jurisdiction over a programmer residing outside of the state's or the country's borders.

{58} Just as computer viruses evolve, so must legislation. State legislators have demonstrated a more aggressive approach to combating cyber-criminals. Since the prosecution of computer crime has been left largely up to the federal government, Congress should follow the states’ lead. Federal, state and international laws addressing computer viruses must: (1) provide a clear and concise definition of a computer virus; (2) provide for harsher penalties for those programmers who are caught; (3) provide a less stringent standard of culpability so programmers do not escape prosecution due to loopholes in the law; and (4) focus on a collaborative effort among all levels of government, the private sector and the international community to bring computer virus authors to justice.

{59} Finally, the curtailment of computer crime will not be a result of punishing individual virus spreaders through the criminal justice system, but can be achieved through requiring the private sector and corporations to tighten their security systems to prevent contamination. The private sector and its employees will be forced to take greater precautions in preventing the spread of computer virus crime because plaintiffs will be able to hold corporations civilly liable for their negligence.

ENDNOTES

[*]. Mark R. Colombell earned a B.S. from the College of Integrated Science & Technology in 1999 from James Madison University, and will received his J.D. in May 2002 from the University of Richmond School of Law. He is currently the Notes & Comments Editor of the Richmond Journal of Law & Technology. Mr. Colombell would like to thank the Journal of Law & Technology staff and Professor Timothy Coggins for providing editorial and critical reviews of this comment. Mr. Colombell would finally like to thank his family and friends for their support throughout law school.

[1]. Patrick Brethour, *E-mails and Virus Slow Web*, The Globe and Mail, Sept. 22, 2001, at B1.

[2]. Michael Bordera, *The Computer Virus War: Is the Legal System Fighting or Surrendering?*, Computers & the Law Project ¶ 1 (1997).

[3]. Quoting the *Ask Jeeves* website *at* http://www.askjeeves.com (last visited Nov. 28, 2001).

[4]. A simple virus is dangerous because it will quickly use all available memory and crash the system.

[5]. Bordera, *supra* note 2, ¶ 2.

[6]. *See id.*

[7]. *See* Robert J. Malone & Reuven R. Levary, *Computer Viruses: Legal Aspects*, 4 U. Miami Bus. L. Rev. 125, 140 (1994) (discussing how Congress, in 1984, passed the Counterfeit Access Device and Computer Fraud and Abuse Act, which was the first legislation addressing computer crime).

[8]. *Id.* at 128.

[9]. *See* Daniel J. Kluth, *The Computer Virus Threat: A Survey of Current Criminal Statutes*, 13 Hamline L. Rev. 297, 299 (1990) (discussing viruses in the human body).

[10]. Malone & Levary, *supra* note 7, at 128.

[11]. *Id.* at 129; *see generally* Kluth, *supra* note 9, at 298 (discussing hidden programming codes and the origin of computer virus terminology).

[12]. Malone & Levary, *supra* note 7, at 129 (defining this constant spreading as the replication process).

[13]. *See id.*; Raymond Hansen, *The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues*, 3 Software L.J. 717, 734 n.76 (1990).

[14]. Malone & Levary, *supra* note 7, at 129; *see also* Bordera, *supra* note 2, ¶ 3 (referencing the Universal Message of Peace virus, that spread on March 2, 1988, as a benign virus).

[15]. *See CKNOW.COM Virus Tutorial: What Viruses Infect*, *at*

http://www.cknow.com/vtutor/vtwhatinfect.htm (last modified Oct. 3, 2001).

[16]. *Id.* System sector viruses infect control information on the disk itself. *Id.*

[17]. *Id.* File viruses infect program files. *Id.*

[18]. *Id.* Macro viruses infect files typically thought of as data files, however, since these files contain macro programs, they can be infected. *Id.*

[19]. *Id.* Companion viruses add files that run to the disk first. *Id.*

[20]. *Id.* Cluster viruses infect the computer through the disk directory. *Id.*

[21]. *Id.* Batch file viruses use text batch files to infect the host computer. *Id.*

[22]. *Id.* Source code viruses cause problems by adding code to the actual program source code. *Id.*

[23]. *Id.* Visual Basic Worms use the Visual Basic language to control the computer and perform tasks. *Id.*

[24]. *See* Malone & Levary, *supra* note 7, at 129.

[25]. *See* Kluth, *supra* note 9, at 300.

[26]. *See id.* (discussing beneficial functions of worm programs, such as being used by the computer to recognize idle computers on the network).

[27]. *See* Bordera, *supra* note 2, ¶ 5 (citing Richard Denning, *Computer Viruses*, 76 AM.SCIENTIST 236 (1988)).

[28].Malone & Levary, *supra* note 7, at 133. *See generally* United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

[29]. Kluth, *supra* note 9, at 300.

[30]. *See* Malone & Levary, *supra* note 7, at 133.

[31]. Bordera, *supra* note 2, ¶ 8 (discussing the manner in which Morris programmed the worm to infect other computers). Morris designed the program to ask each computer whether it had already been infected. If the computer returned a negative response, the worm would then infect that computer. Morris thought even more steps ahead by predicting how often a computer would falsely respond affirmatively, so he programmed the worm to duplicate itself after every seventh affirmative response. *Id.*

[32]. *Id.* (stating that the Defense Department purposely designed flaws in the e-mail system to allow for easy access and repairs).

[33]. *See* United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991).

[34]. *See* Kluth, *supra* note 9, at 301.

[35]. Cox News Service, *150,000 Web Sites Invaded: Worm to Launch Attacks on Net in Mid-August*, RICH. TIMES DISPATCH, Aug. 2, 2001, at A1.

[36]. *Id.*

[37]. *See* Kluth, *supra* note 9, at 301.

[38]. *See* Malone & Levary, *supra* note 7, at 139.

[39]. *See* Kluth, *supra* note 9, at 298.

[40]. *See id*. (discussing how a Trojan horse program could serve the function of destroying hardware, software, data or could simply be a means of transferring the virus).

[41]. Bordera, *supra* note 2, ¶ 5.

[42]. *Id*. (discussing that a logic bomb program could be set to detonate based on the number of times a program is run or a certain date)

[43].*CKNOW.COM* Virus Tutorial *at* http://www.cknow.com/vtutor/vtlogicbomb.htm.

[44]. *Id*.

[45]. *Id*.

[46]. *Id*.

[47]. *Id*.

[48]. *Id*. (discussing concern raised by the Macro virus in the legal field).

[49].Bordera, *supra* note 2, ¶ 6.

[50]. *Id*. (discussing concern raised by the Macro virus in the legal field).

[51]. *See* Brethour, *supra* note 1.

[52]. *Id*. Nimda uses e-mail attachments to replicate itself, like the Melissa virus, and spreads itself through infected Web servers, like the Code Red worm. *Id*.

[53]. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. § 1030 (2000)).

[54]. *See* Malone & Levary, *supra* note 7, at 140.

[55]. Literary reference to George Orwell's classic novel "1984", which comments on the dangers of technology.

[56]. *See* Malone & Levary, *supra* note 7, at 140-41 (discussing lobbying efforts for passage of the Counterfeit Access Device and Computer Fraud and Abuse Act).

[57]. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, *supra* note 50.

[58]. The Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030(a)(5) (2000)).

[59]. 18 U.S.C. § 1030(a)(5) (2000).

[60]. *See supra* Part II-D.

[61]. Bordera, *supra* note 2, ¶ 9.

[62].18 U.S.C. § 1030(a)(1) (2000).

[63]. *Id.*§ 1030(a)(2) (2000).

[64]. *Id.* § 1030(a)(3) (2000).

[65]. *Id.* § 1030(a)(4) (2000).

[66]. *Id.* § 1030(a)(5) (2000).

[67]. *Id.* § 1030(a)(6) (2000).

[68]. Bordera, *supra* note 2, ¶ 1.

[69]. *Id.*

[70]. *Id.* ¶ 10.

[71]. *Id.*

[72]. *Id.* ¶ 9.

[73]. *Id.* ¶ 17.

[74]. *See id.* ¶ 9 (discussing the efforts of Congressman Herger of California, who headed the bill and recognized the deficiency in computer crime prosecution).

[75]. *See id.* ¶ 14 (discussing the proposed bill that was introduced as H.R. 55 during the 101st session of Congress).

[76]. *See id.* ¶ 13 (discussing the loopholes in the 1986 Act). Programmers could escape prosecution by (1) having authorization to be working on a computer network; (2) not having his virus affect computers owned by the government; (3) not causing damage in excess of $1000.

[77]. The Computer Virus Eradication Act of 1989, H.R. 55, 101st Cong. § 2(a)(3) (1989).

[78]. *See* Bordera, *supra* note 2, ¶ 12.

[79]. *Id.* ¶ 13.

[80]. The Computer Virus Eradication Act of 1989, H.R. 55, 101st Cong. § 7 (1989).

[81]. Kelly Cesare, Comment, *Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution,* 14 TRANSNAT'L LAW. 135, 146 (2001).

[82]. The National Information Infrastructure Protection Act § 1030(a)(5)(A)(i) (1996). NIIPA was recently changed by the USA PATRIOT ACT. Changes are reflected in this paper and in this footnote.

[83]. NIIPA, §§ 1030(a)(5)(A)(ii), (iii) (1996).

[84]. *See* Cesare, *supra* note 81, at 147 n. 92 (citing Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 217 (2000)).

[85]. Sections of NIIPA have eliminated some possible defenses for computer virus authors regarding jurisdiction, intent, and the amount of damage required to be inflicted.

[86]. Editorial, *A Defense for the Internet: Threat to Nation: White House Acts on Cyber Security to Lessen U.S. Vulnerability to Terrorism,* BALT. SUN, Oct. 10, 2001, at 16A.

[87]. *Id.*

[88]. *Id.*

[89]. Stephen Barr, *FBI Alert Sends a Wave of Anxiety Through the Workplace*, WASH. POST, Oct. 14, 2001, at C2.

[90]. David Radin*, Are Cyber Viruses Part of Terrorists' Overall Scheme?,* PITT. POST-GAZETTE, Nov. 1, 2001, at E2.

[91]. *Id.*

[92]. Editorial, *supra* note 86.

[93]. *Id.*

[94]. *See* Bordera, *supra* note 2, ¶ 16.

[95]. *See generally id.* (source lists and, in some instances, describes recent statutory enactments of 49 U.S. states).

[96]. ME. REV. STAT. ANN. tit. 17-A, § 431 (West Supp. 1996).

[97]. OKLA. STAT. ANN. tit. 21, §§ 1951-1955 (West Supp. 1998).

[98]. Xan Raskin & Jeannie Schaldach-Paiva, *Computer Crimes*, 33 AM. CRIM. L. REV. 541, 569 (1996).

[99]. *Id.* at 570 (citing Ulrich Sieber, *Computer Crimes and Other Crimes Against Information Technology: Commentary and Preparatory Questions for the Colloquium of the Association Internationale de Droit Penal in Wurzburg*, 64 REV. INT'L DE D. PENAL 67 (1993)).

[100]. *See* Cesare, *supra* note 81, at 150.

[101]. *Id.* at 152.

[102]. *Id.*

[103]. *Id.*

[104]. *Id.*

[105]. *See id.* at 143, 152.

[106]. *See* Damien Whitworth & Dominic Kennedy, *Author Could Escape Arm of the Law*, TIMES (London),

May 5, 2000, Ed. 4M at 10.

[107]. *See* Cesare, *supra* note 81, at 144.

[108]. *Id*. at 152.

[109]. *Id*. at 153.

[110]. *Id*.

[111]. *Id*.

[112]. *Id*. at 154.

[113]. *Id*.

[114]. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[115]. *See* Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (1996).

[116]. 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, 176 (1997).

[117]. *See id*. (explaining that contract law was used as the basis of recovery for computer crimes, because the loss was almost exclusively economic, and courts have denied negligence claims for purely economic reasons).

[118]. In *People Express Airlines, Inc. v. Consol. Rail Corp*., 495 A.2d 107, 118 (N.J. 1985), the court held that "a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty."

[119]. Robin A. Brooks, Note, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the "Net"?*, 17 REV. LITIG. 343, 357-58 (1998).

[120]. *Id*. at 358.

[121]. *Id*. at 359. Employers that could be held potentially liable are software companies, Internet service providers, bulletin board systems operators, or data repositories. *Id*.

[122]. *See id*.

[123]. *See id*.

[124]. *See* Gripman, *supra* note 115, at 179.

[125]. *See id*.

[126]. *Id*.at 179-80.

[127]. *See id*.at 180.

[128]. *See id*.

[129]. *See id*.

[130]. *Id*. at 181.

[131]. Michael Millington, *Virus Alert: Is Your Computer Next?*, Colo. Law., May 28, 1999, at 47, 48 (1999) (noting several of the largest software packages for computer virus prevention and detection are McAfee's VirusScan and Symantec's Norton AntiVirus).

[132]. "A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that, considering the nature and purpose of he actor's conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation." BLACK'S LAW DICTIONARY, 1270 (6th ed. 1990).

Related Browsing

1. http://special.northernlight.com/compvirus/index.html Divine RivalEye provides a comprehensive database of websites containing information on computer viruses to include sections on current news, diagnostics, government resources, and anti-virus solutions.

2. http://securityresponse.symantec.com/avcenter/vinfodb.html/ Symantec is one of the major developers of anti-virus software. This portion of their website provides descriptions for many past and present computer viruses.

3. http://www.digitalcentury.com/encyclo/update/comfraud.html The Computer Fraud and Abuse Act of 1986 was signed into law in order to clarify definitions of criminal fraud and abuse for federal computer crimes and to remove the legal ambiguities and obstacles to prosecuting these crimes. The Act established two new felony offenses for the unauthorized access of "federal interest" computers and a misdemeanor for unauthorized trafficking in computer passwords.

4. http://fedlaw.gsa.gov/legal8.htm Links to federal statutes and regulation pertinent computer and information technology law.

5. http://www.ussc.gov/publicat/cmptfrd.pdf U.S. Sentencing Commission, Summary Report of Findings of the Computer Fraud Working Group. This report addresses whether computer fraud offenses, codified at 18 U.S.C. § 1030, are sufficiently distinct from fraud offenses to justify development of separate sentencing guidelines.