Richmond Journal of Law and Technology

Volume 6 | Issue 5 Article 4

2000

The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?

Jeff Nemerofsky

Volume VI, Issue 5, Spring 2000

The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?

Jeff Nemerofsky[*]

Cite As: Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?*, 6 RICH. J.L. & TECH. 23 (Spring 2000) <http://www.richmond.edu/jolt/v6i5/article2.html>. [**]

TABLE OF CONTENTS

I. INTRODUCTION

{1}The "interruption of computer services to authorized users," involves a violation of a series of federal and state computer-related crime laws which are designed to protect the authorized users of computer systems.[1] Because most of these laws have only recently been legislated, and since few people have ever actually been charged with such violations, there is very little history or case law in this area. However, as computer-related crimes continue to escalate, these statutes could prove to be a positive force in efforts to catch the electronic criminals of the future. "Although there has never been accurate nationwide reporting of computer crime, it is clear from the reports which do exist . . . that computer crime is on the rise."[2] As a matter of fact, between January 1998 and December 1998, the Computer Emergency and Response Team Coordination Center (CERT/CC)[3] received "41,871 e-mail messages and 1,001 hotline calls reporting computer security incidents or requesting information."[4] In addition, they received 262 vulnerability reports and handled 3,734 computer security incidents, affecting more than 18,990 sites during this same period.[5]

{2} At first blush, one might think that a statute to protect authorized users of computer systems from any interruptions in their service would be aimed at preventing large computer service providers such as America Online or Compuserve from illegally cutting off one's monthly access. Thus, these statutes *appear* to be related more to the laws of contracts and the enforcement of one's rights under a valid agreement between a computer user and service providers. In reality, these laws have nothing to do with contracts and everything to do with catching those who attempt to disrupt computer software and systems.

{3} Typically, laws that attempt to convict "hackers,"[6] or those who insert a "virus"[7] into a system, do so by charging the perpetrator with computer trespass, illegal access, unauthorized use or computer contamination.[8] The purpose of this article is to introduce and explain another method for convicting those would-be computer intruders, rules which are already in place at the state level,[9] and possibly the federal level as well. The crime of "interruption of computer services to authorized users" occurs when a perpetrator denies or degrades computer services to another user who has proper authorization. Sometimes, the perpetrator's main objective is to do nothing more than interrupt or deny another user from accessing the system. This is done by way of "denial-of-service" programs which aim to shut down a targeted system by sneaking or barging in and overwhelming it.[10]

{4} The intentional or even accidental interruption of computer services caused by the service provider itself upon its own users will not be the focus of this comment, since those issues would invariably be covered by an existing contract between the parties. Instead, this comment will address the criminal liability of a

computer user who interrupts the services of either the provider of those services or other remote authorized users of that system.

II. BACKGROUND

A. *Interrupting Whom - The Service Providers or the Users?*

{5} The "interruption of computer services" crime is limited to "authorized users" in order to differentiate two interpretations of the first part of that phrase, "interruption of computer services." A law that makes it a crime to "interrupt computer services" may be directed at protecting either the provider of those computer services *or* the users of that system. For instance, if a perpetrator causes an interruption of computer services, the mainframe provider of those services may have a cause of action against the perpetrator for the disruption to their system. On the other hand, if the law is directed towards other remote authorized users of the system, then those users may have a cause of action against the perpetrator for any damages suffered as a result of a degradation in their access caused by the perpetrator's interruption.

{6} This dual interpretation of the law is further muddled by the fact that many federal and state statutes refer only to the crime as an "interruption of computer services," and no more.[11] Thus, the statutory language provides no additional insight as to the legislators' intent. For example, is the law meant to protect service providers of computer systems, authorized users of those systems, or both? Speaking generally, there is no reason why the provider of computer services cannot be considered an authorized user of its own system. This still leaves open to interpretation, however, precisely *whom* the law is intended to protect. Upon closer examination, these statutes raise a multiplicity of issues concerning problems of inclusion and jurisdiction not immediately cognizable. The following case delineates the two types of "interruptions" that are discussed above.

{7} In *Briggs v. State*,[12] the court analyzed how its state statute would deal with the first type of interruption- disruption inflicted on the service provider itself. The Scarborough Group, a securities investment company, hired Terry Briggs, a twenty-three year old computer specialist, to program and design software to maintain an investment company's computer system.[13] Nine months later, Briggs resigned as a result of a dispute about the terms of his employment contract.[14] Before leaving, Briggs "secured" some of the company's computer files with passwords known only to him.[15] "The State alleged that Briggs intentionally and willfully and without authorization accessed a computer system to interrupt the operation of the computer system and computer services."[16] This scenario would appear to represent the first interpretation of the term "interruption," which is the disruption inflicted upon the service provider itself.

{8} However, in discussing how various states have explicitly prohibited computer use to unauthorized users, the court noted that "several states have specific offenses entitled 'offenses against computer users,' which criminalize the intentional denial to an authorized user of the full and effective use of or access to a computer."[17] In doing so, the court also identified an alternative interpretation of "interruption:" disruption of computer services to the authorized users of the system.

B. *Denial-of-Service Attacks*

{9} A "denial-of-service attack" (commonly referred to as a DoS Attack) is an attack or intrusion designed for use against computers connected to the Internet[18] whereby one user can deny service to other legitimate users[19] simply by flooding the site with so much useless traffic[20] that no other traffic can get in or out. In fact, the "hacker" isn't necessarily trying to break into the system or steal data, but rather just prevent users from accessing their own network[21] for reasons only the hacker knows: revenge, economical or political gain, or just plain nastiness![22] For example, consider the possibility of customers being turned away from

an electronic catalog at Christmas time.[23] As will be discussed later in further detail, these interruptions may be deliberate or accidental, however, a denial of service attack is considered to take place only when access to a computer or network is intentionally blocked as a result of some malicious action.[24]

{10} There are several ways a denial of service attack may occur--service overloading and message flooding are but two[25]-- and these attacks may be directed against either a user, a host computer, or a network.[26] These attacks have a vernacular all their own and can be categorized as "fork bombs," "malloc bombs," "SYN flood" and "mail bombs,"[27] with specific names such as "Ping of Death," "Teardrop,"[28] "Boink," "New Tear" and "IceNewk."[29] For instance, one attack paints a huge black window on the user's screen in such a way that the user can no longer access the remainder of their screen.[30]

{11} According to a recent press release from the U.S. Department of Justice, Eugene F. Kashpureff pleaded guilty to unleashing software on the Internet that interrupted service to tens of thousands of users worldwide.[31] Kashpureff re-routed Internet users that were attempting to reach the website of his chief commercial competitor and hijacked them to his own website.[32] Similarly, officials brought criminal charges against a hacker who sent a series of disabling computer commands to the telephone company that serviced the community of Rutland, Massachusetts, including the Worcester Airport.[33] The outage disabled vital services to the Federal Aviation Administration control tower for six hours.[34]

III. ANALYSIS

A. *Perspective*

1. Federal Computer Crime Laws

{12} Does the crime of an "interruption of computer services to authorized users" even exist on the federal level? A closer look at some of the original federal computer crime statutes will help shed some light on the answer to that question. An examination of these laws is also relevant for purposes of identifying factors which impact computer crime legislation at the state level.

a. The Computer Fraud and Abuse Act - 1984, 1986

{13} In 1984, in response to the growing wave of computer crime, Congress enacted the first federal computer crime statute, the Counterfeit Access Device and Computer Fraud and Abuse Act.[35] Congress was reluctant to preempt or interfere with the local and state computer crime authorities, and therefore, these early versions of federal computer crime legislation protected only a relatively narrow class of government operated computers.[36] The Act made it a felony to knowingly access a computer without authorization in order to obtain classified defense information with the intent that such information would be used to harm the United States.[37] In addition, the 1984 Act made it a misdemeanor to knowingly access a computer without authorization in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency, or to use, modify, destroy, or disclose information in a computer operated on behalf of the United States if such conduct would affect the government's use of the computer.[38]

{14} Two years later, Congress amended the 1984 Act by creating the 1986 Computer Fraud and Abuse Act (CFAA).[39] That amendment eliminated some of the prior Act's confusing language, defined additional terms and expanded the scope of the 1984 Act by including three additional types of computer crimes: a computer fraud offense patterned after the federal mail and wire fraud statutes; an offense for the alteration, damage or destruction of information contained in a "federal interest computer"; and an offense for the trafficking of unauthorized computer passwords in certain circumstances.[40]

i. Section (a)(5)

{15} The 1986 Amendment to the 1984 Act added the following section, which was concerned with the intentional access and unauthorized use of a government computer.

> (a) Whoever-- (5) intentionally accesses a Federal interest computer[41] without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use of any such computer* (emphasis added) or information, and thereby-- (A) causes loss to one or more others of a value aggregating $1,000 or more . . . shall be punished . . . .[42]

{16} As can be seen, there is no provision specifically relating to the crime of an "interruption of computer services to authorized users," however, section (a)(5) above does make it a crime for anyone who "*prevents authorized use of any such computer*. . . ."[43] Under a liberal interpretation of that phrase, one could easily define the statute's "prevention" of authorized use as an "interruption" of that use. But, it is unclear as to whom the statute's prevention of authorized use is directed. On the one hand, the statute may be interpreted as making it a crime for one to prevent the providers of computer systems from delivering uninterrupted services to their authorized users. Or, the statute may be seen as making it illegal for one who "prevents [the] authorized use" of other authorized users. Does it really matter?

{17} In fact, under the 1986 Act, the distinction between the prevention of use to providers or users probably does not make much of a difference. That is because the amendment covers only government computers,[44] and under that scenario, the user and the provider are generally one and the same due to the fact that those using government computers are invariably employees, agents or contractors of the government.

{18} The following case represents one of the few occasions where anyone has been prosecuted under section (a)(5) of the Computer Fraud and Abuse Act.[45]

ii. United States v. Morris

{19} Perhaps the most infamous Internet crime ever committed was the 1988 case of *United States v. Morris*.[46] Robert Tappan Morris was a 23 year-old first year graduate student in Cornell University's computer science Ph.D. program[47] and through various jobs, had acquired quite a significant amount of computer experience. Morris was given an account on his school's computer, and soon began work on a computer program, later known as the INTERNET "worm" or "virus."[48] Morris intended to release the worm into university, government, and military computers around the country in order to demonstrate the inadequacies of current security measures on those computer networks.[49] "The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of those computers."[50]

{20} After releasing his "harmless" worm, Morris soon discovered that it was actually infecting machines, ultimately causing computers at over 6,000[51] educational institutions and military sites around the country to "crash" or cease functioning.[52] With the help of a friend, Morris then sent out an anonymous message instructing programmers how to kill the worm and prevent re-infection. But "because the network route was clogged, the message did not get through until it was too late."[53] Morris was found guilty of violating the Computer Fraud and Abuse Act, Section 1030(a)(5)(A), which prohibited intentional unauthorized access to federal computers.[54] "He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision."[55]

{21} As previously cited, section 1030(a)(5) of the 1986 Computer Fraud and Abuse Act covered anyone who "intentionally accesses a Federal interest computer without authorization, and by means of one or more

instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information. . . . "[56]

{22} Morris's defense was that although he *did* intend to access the network without authorization, he did *not* intentionally wish to cause any damage.[57] In other words, Morris argued that the adverb "intentionally" modified *both* verb phrases of the section above, and that the Government had to prove not only that he "intentionally" accessed a federal computer, but also that he "intentionally" altered information or prevented authorized use.[58]

{23} The Second Circuit Court of Appeals agreed with the district court's conclusion that the intent requirement applied only to the act of accessing the system, and not to the alteration of information or the prevention of authorized use.[59] In making their finding, the Second Circuit quoted a report of the Senate Judiciary Committee that concluded, "(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."[60] This would suggest that Congress was principally concerned with the act of entering the system, rather than the resulting destruction of information.

{24} The holding of the *Morris* case is important to the present discussion because, as will be discussed later, the "intentional" standard resurfaces again in a number of statutes which protect authorized computer users against those who interrupt their service.

{25} Although the Second Circuit Court of Appeals found that there was sufficient evidence for the jury to conclude that Morris acted "without authorization" within the meaning of Section 1030(a)(5)(A),[61] the facts stated in the court's opinion in *Morris* do not indicate whether Morris was technically charged with the prevention of "authorized use of any such computer" under section (a)(5).[62] However, it appears obvious that he very well could have. Thus, an "interruption of computer services to authorized users," as I refer to it, could have also been invoked to implicate Morris for his crimes.

b. The Computer Abuse Amendments Act - 1994

{26} In 1994, Congress amended the 1986 Computer Fraud and Abuse Act to broaden the federal law as it related to computer "worms" and "viruses."[63] The 1994 Computer Abuse Amendments Act was actually the smaller part of a more comprehensive omnibus crime bill entitled "The Violent Crime Control and Law Enforcement Act of 1994"[64] which President Clinton signed into law on September 13, 1994. Specifically, three changes were made to section 1030 (a)(5): coverage of the Act was expanded to include computers used in interstate commerce; the requirement of an "unauthorized access" was removed which meant that company insiders and authorized users could be held liable; certain types of reckless[65] conduct and intentional[66] acts were deemed criminal.[67] Section 1030 (a)(5)(A) read in part as follows:

> (a) Whoever-- (5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of program, information, code, or command to computer or computer system if- (i) the person causing the transmission intends that such transmission will- (I) damage, or cause damage to, a computer, computer system, network information, data, or program; or (II) withhold or deny, or cause the *withholding or denial, of the use of a computer*, computer services, system or network, information, data, or program; and
>
> > (ii) the transmission of the harmful component of the program, information, code, or command-
> >
> > > (I) occurred without the authorization of the persons or

> entities who own or are responsible for the computer system receiving the program, information, code, or command; and
>
> (II)(a) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period; . . . shall be punished . . . .[68]

{27} Again, there was no language in the statute specifically referring to the crime of an "interruption of computer service to authorized users."[69] However, section (a)(5)(i)(II) listed above does appear to be the most relevant location for arguing the existence of such a law, if indeed one exists on the federal level. The above mentioned section uses the phrase *"withholding or denial of the use of a computer*"[70] which could also be easily interpreted as an "interruption" of the use of that computer by others.

c. The Computer Fraud and Abuse Act as Amended by the National Information Infrastructure Protection Act of 1996

i. Section 1030 (a)(5)

{28} Because Congress determined that the scope of the 1994 Act was still too limited, Senators Leahy,[71] Kyl and Grassley along with Representatives McCollum, Schumer and Hamilton sponsored an amendment to the Act entitled the National Information Infrastructure Protection Act (NIIPA) of 1996.[72] When originally introduced in 1995, the NIIPA failed to emerge from the Judiciary Committee proceedings.[73] However, on October 11, 1996 President Clinton signed into law the NIIPA of 1996,[74] which was enacted under the same bill (H.R. 3723) as the Economic Espionage Act of 1996.[75] The purpose of the amendment was to include computers in the private sector (called protected computers[76]) as well as those under government domain.[77] Section 1030 (a)(5), in its current form reads in part as follows:

> (a) Whoever-- (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally *causes damage* (emphasis added) without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; . . shall be punished. . . .[78]

{29} Much has been written about the drastic changes made to the structure of this section and the inclusion of three different "mens rea" requirements---the mental state component required for committing particular crimes, which came about as a result of the case of *United States v. Morris*.[79] Essentially, the amendment "provides that individuals who access protected computers without authority are responsible for the consequences of their actions [intentional, reckless, or negligent[80], but those accessing with authority are criminally liable only if they intend to cause damage to the victim."[81] However, virtually nothing has been written about the elimination of subsection (a)(5)(A)(i)(II) of the 1994 Act which charged one with a crime for "withholding or denial of the use of a computer."[82] That was the language which appeared most appropriate for identifying the crime of an "interruption of computer services to authorized users."

{30} Today, under the current statutory scheme, one wishing to bring federal charges for the same "interruption of computer services" crime would most likely have to do so under section (a)(5)(A), (B) or (C) of the 1996 Act. Those sections state that whoever knowingly causes the transmission of a program or intentionally accesses a protected computer and "*causes damage*" shall be punished.[83] However, the term

"causes damage" does not appear to lend itself nearly as well to the transliteration of an "interruption" of computer services as did the "withholding" or "denial" language of former section (a)(5)(A)(i)(II) of the 1994 Act.

{31} As already mentioned, it is also important to note that the 1999 statute now covers protected computers, [84] or computers no longer strictly under government domain. Therefore, the comment alluded to previously,[85] that the statute was not really designed to protect authorized users since users and providers of the system were essentially the same entity (government), is no longer applicable. With the Act's expanded coverage to private computers, the distinction between provider and user is more clear, and the term "causes damage" could refer to injuries suffered by either provider or user.

{32} In 1998, America Online (AOL) brought a complaint against LCGN, Inc. for sending out large numbers of unauthorized and unsolicited bulk e-mail advertisements to AOL members.[86] The court noted that, "[t]he undisputed facts establish that defendants violated 18 U.S.C. section 1030(a)(5)(C) of the Computer Fraud and Abuse Act, which prohibits anyone from 'intentionally access[ing] a protected computer without authorization, and as a result of such conduct, causes damage.'"[87] Although America Online was successful in their action, they probably could have also argued that the crime of an "interruption of computer services" was committed under a liberal interpretation of section 1030(a)(5)(C).

ii. Section 1030 (a)(3)

{33} Another provision of the CFAA that is relevant to any discussion of an "interruption of computer services" crime is section 1030(a)(3) which reads as follows:

> (a) Whoever-- (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct *affects* (emphasis added) [88] that use by or for the Government of the United States; . . . shall be punished . . . .[89]

{34} Section 1030 (a)(3) is generally regarded as a "pure trespass provision."[90] However, under a very liberal interpretation of this section, one who intentionally accesses a government computer without proper authorization may "affect" another authorized user of that system such that, it could be considered an interference or disruption of that user's service. Although this situation may be considered an unlikely scenario and a "stretch" in statutory translation, it may still provide a way to implicate one who has interfered in someone else's legitimate receipt of computer services. However, a first violation of section 1030 (a)(3) is always a misdemeanor offense,[91] which might not provide enough dissuasion or disincentive to prevent a potential criminal from attempting such an illegal act.

2. Must There be Intent to Access/Cause Damage?

a. Authorized Access / Unintentional Damage

{35} Suppose person "A," an authorized user of American Online (AOL), receives an e-mail message from a friend, but does not know that the message also contains a hidden computer virus. Person "A" then forwards that electronic message to another friend which causes the virus to activate and spread throughout the system. If the system is so degraded that service is disrupted or even shut down, is person "A" guilty of the crime of "interruption of computer services" (providing of course that the AOL is not negligent for failing to exercise

reasonable care in utilizing some type of virus scanning mechanism to detect or "proofread" messages before they are sent[92])? Person "A" did not intend to transmit the virus to another computer when sending the e-mail, but only intended to transmit the message itself. Under the current version of the Computer Fraud and Abuse Act,[93] Person "A" would probably not be guilty of any crime since there was no intent to transmit the virus. "Whether authorized users should ever be criminally liable for reckless damage is [another] debatable question. For example, it could be deemed reckless in today's computer environment to intentionally copy a file from a floppy diskette to a hard drive without first running a virus scan--although imposing criminal sanctions for such conduct is clearly inappropriate, absent other criminal intent."[94]

b. Unauthorized Access / Unintentional Damage

{36} In an article by Marc S. Friedman and Kristin Bissinger, presented by Mary J. Hildebrand,[95] an interesting scenario is hypothesized with regards to an interruption of computer services. As previously discussed in *United States v. Morris*,[96] Robert Morris was an authorized user of the Cornell University computer system, but trespassed onto federal computers when he released his "harmless" worm into the national computer network.[97] After learning that his worm was actually damaging machines, Morris attempted to send a message to programmers on how to kill the worm, or in effect, create an antidote worm.[98] Thus, one who knowingly invades a system without authority and causes significant loss to the victim should be punished even when the damage caused is not intentional. "To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, they commit no crime unless that damage was either intentional or reckless."[99] In fact, the purpose of the 1996 amendment to section 1030 (a)(5) of the Computer Fraud and Abuse Act[100] was to restore criminal liability for such behavior.

{37} Friedman and Bissinger note that Morris' antidote worm raises the question of whether all worms or viruses are evil, and should be prohibited. "For example, software vendors might want to release a 'good' worm which looks for and reports suspicious activity, such as the caching of pirated software."[101] Such a worm would theoretically consume system resources, thereby interrupting service to authorized users. The question is whether such an activity would be illegal under statutes making it a crime to deny or interrupt computer services to authorized users. The authors note that there is already a legitimate program called, Security Analysis Tool for Auditing Networks ("SATAN") which attempts to breach security devices. SATAN is intended to be used by system administrators to expose security flaws in networks.[102]

{38} Stevan D. Mitchell and Elizabeth A. Banker, in their article entitled, "Private Intrusion Response"[103] noted a similar program created by telecommunications giant, MCI. MCI announced it's intent to release free software that could track down "hackers"[104] by following paths back through several servers to locate the source of the attack.[105] Are SATAN's authors or MCI's system programmers guilty of the crime of an "interruption of computer services" for intentionally releasing beneficial computer programs that may have the debilitating effect of interrupting services to authorized users?

3. Catching the Criminal

a. Prosecution

{39} Several theories abound regarding why there are so few people actually caught and convicted for the crime of an "interruption of computer services."[106] One theory may lie in the difficulty of valuing just how "much" of an interruption has actually occurred to an authorized user. Small or insignificant disruptions in service may be non-actionable under the legal doctrine of "de minimis non curat lex."[107] Such was the case in *Feinman v. Bank of Delaware*.[108] In *Feinman*, which could be considered a case of an "interruption of computer services to authorized users," a bank temporarily denied a customer's access to his money through

automated teller machines due to an overdraft in his account. The customer filed suit when the bank, due to either unintentional human error or a computer glitch, did not promptly remove the restrictions.[109] The court held that the customer failed to prove actual damages for the short period of time (2 days) that he was unable to withdraw money from the ATM because he still retained the ability to access funds either by writing checks or through human teller withdrawals.[110] Another "interruption" type of scenario in which damages may be hard to quantify is described by the Criminal Division of the U.S. Department of Justice:

> Computer intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information has been damaged. Nonetheless, the intruder's conduct allowed him to accumulate valid user passwords to the system, required all system users to change their passwords, and required the system administrator to devote resources to resecuring the system. Thus, although there may be no permanent "damage," the victim does suffer "loss." [111]

As a result, law enforcement officials may have more incentive to prosecute criminals for such crimes as theft, embezzlement and receipt of stolen computer property whereupon valuation of such items may be easier to determine and where sentencing guidelines for those crimes may potentially be more severe.

{40} Under section 1030(e) of the current Computer Fraud and Abuse Act:

> (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that-- (A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals; (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (C) causes physical injury to any person; or (D) threatens public health or safety[112]

{41} Although the word "damage" is now defined more broadly than was the case under the 1986 Computer Fraud and Abuse Act which listed specific prohibited acts that could have caused impairment to data and systems (such as "alters, damages or destroys information"[113]), and which thus limited the scope of the previous Act, it is still a nebulous term. Direct damage in excess of $5,000 as a result of an interruption of computer services may still be difficult to quantify if no files are destroyed, no software is ruined and no classified systems are compromised.

{42} Nevertheless, the U.S. Department of Justice notes that even though a number of computer crimes have been charged under a host of other criminal statutes, they believe that much of that criminal behavior could have been successfully prosecuted under the Computer Fraud and Abuse Act.[114]

b. Sentencing

i. Federal

{43} Another possible theory for the low number of prosecutions for those who interrupt the computer services of others may be related to the relatively light sentences sanctioned for such offenses. With regards to punishment under section 1030 (a)(5) of the Computer Fraud and Abuse Act, section (c) of the Act states in part:

> (c) The punishment for an offense under subsection (a) or (b) of this section is-- . . . .

(2)(A) a fine under this title or imprisonment for not more than one year, or both,in the case of an offense under subsection . . . (a)(5)(C), ... (3)(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection . . .(a)(5)(A), (a)(5)(B).[115]

{44} As previously noted in section 1030 (a)(5), the nature of an offense is determined by the mental state of the perpetrator, namely whether the actions were intentional, reckless or negligent. Per section (c) above, intentional or reckless damage caused by an unauthorized user (trespasser), is punishable as a felony as is the intentional damage caused by an authorized user. However, an authorized user who negligently causes damage is guilty of only a misdemeanor and could conceivably receive a punishment of just 6 months in jail[116] and a small fine.[117] Of course, the disposition of any case depends on which specific prohibited acts were committed and the particularity of the circumstances involved.[118]

{45} In determining the effect circumstances may have on the specific punishment to be imposed, the United States Code includes Chapter 227, Subchapter A--General Provisions[119] which identifies several factors the court shall consider in determining an individual sentence.

Section 3553. Imposition of a sentence

. . . . (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed-- (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;

(3) the kinds of sentences available;

(4) the kinds of sentence and the sentencing range established for--

(A) the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines issued by the Sentencing Commission pursuant to section 994(a)(1) of title 28, United States Code, and that are in effect on the date the defendant is sentenced; or

(B) in the case of a violation of probation or supervised release, the applicable guidelines or policy statements issued by the Sentencing Commission pursuant to section 994(a)(3) of title 28, United States Code;

(5) any pertinent policy statement issued by the Sentencing Commission pursuant to 28 U.S.C. Sec. 994(a)(2) that is in effect on the date the defendant is sentenced;

(6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and

(7) the need to provide restitution to any victims of the offense.[120]

ii. State

{46} Many states' criminal statutes no longer retain the historical misdemeanor/felony distinction previously accepted, and instead now classify crimes according to degree.[121] For instance, in Louisiana the computer crime statute relative to authorized computer users reads as follows:

> Section 73.4. Offenses against computer users
>
> A. An offense against computer users is the intentional denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network, or computer services.
>
> B. (1) Whoever commits an offense against computer users shall be fined not more than five hundred dollars, or be imprisoned for not more than six months, or both, for commission of the offense. (2) However, when the damage or loss amounts to a value of five hundred dollars or more, the offender may be fined not more than ten thousand dollars, or imprisoned with or without hard labor, for not more than five years, or both.[122]

{47} As can be seen, there is no mention in the statute of felonies or misdemeanors, but instead, the appropriate punishment is determined by the amount of damage caused by the denial to access or use. Alternatively, some states continue to base their sentencing schemes upon the more traditional classifications of felony and misdemeanor. For instance, Nevada's statute on the unlawful interference with or denial of access or use of a computer states:

> Section 205.477
>
> 1. Except as otherwise provided in subsection 3 (if the violation was committed to devise or execute a scheme to defraud or illegally obtain property), a person who knowingly, willfully and without authorization interferes with, denies or causes the denial of access to or the use of a computer, system or network to a person who has the duty and right to use it is guilty of a misdemeanor.[123]

{48} In either scenario, the punishment for the crime of a denial or "interruption of computer services" tends to be less severe than for one who knowingly or intentionally alters, damages, deletes or destroys computer data, programs or software.[124]

4. Remedies Available to the Victim of an Interruption

a. Civil Damages

{49} At both the federal and state levels, one who commits the crime of an "interruption of computer services to authorized users" may be subject to a civil action[125] as well as criminal penalties under certain circumstances. On the federal level, the Computer Fraud and Abuse Act makes it clear that civil damages are a recognized form of relief. Section 1030(g) of the Act states that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[126] In the previously discussed 1988 case of *United States v. Morris*,[127] none of the victims of Morris' virus could recover civil damages under the Act since there was no provision for such penalties at that time.[128]

{50} On the state level, many statutes include civil relief provisions similar to that of federal law as part of

that state's comprehensive computer crime law.[129] For instance, the Illinois Criminal Code states:

> (c) Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section [the section concerned with losses suffered by computer users] may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses.[130]

{51} By adding these special provisions to the law, the legislature allows the victim of such a crime to potentially receive compensation for his damages without the necessity of an expensive and time consuming lawsuit to prove the existence of a legal doctrine. However, the necessary evidentiary elements still need to be met by the party bringing the action.

b. Tort

{52} One form of civil action available to a victim of an "interruption of computer services" is to sue in "tort." "'Tort' comes from the Latin word 'tortus,' which means twisted, and the French word 'tort,' which means injury or wrong."[131] A tort is a "private or civil wrong or injury, including action for bad faith breach of contract, for which the court will provide a remedy in the form of an action for damages."[132] As a general matter, torts can be divided into several main categories depending on the defendant's state of mind and the nature of his or her conduct.[133] For the purposes of this discussion, only three areas of torts appear to have some connection to the crime of an "interruption of computer services:" (1) intentional torts; (2) tortious interference; and (3) negligence.

i. Intentional Torts

{53} To establish "intentional tort" liability, the plaintiff must prove that a wrongful volitional act was intentionally done by the defendant which caused or was a substantial factor in causing injury to the plaintiff.[134] With regards to the crime of an "interruption of computer services," two potential problems immediately arise concerning these elements. The first dilemma is trying to prove that the defendant intentionally attempted to interrupt the computer services of another remote authorized user. For example, if the defendant's objective is to penetrate a highly secure computer network, and in the process of doing so accidentally interrupts the service to thousands of other remote users, the defendant's specific intent to have caused the interruption may be lacking. However, modern legal thinking is beginning to change the way we view our rights in receiving computer services. If the law deems that the "right" to receive information and computer services by authorized users from mainframe service providers is a "property" interest, the mere fact that the defendant invaded a user's service may be considered a trespass[135] upon each user's "property" or "chattel."[136]

{54} In terms of a trespass to chattel, "[i]t is important to distinguish the intent to do the act from the intent to cause the act's consequences."[137] "The intent required for trespass to chattels ... is simply the intent to do the act that results in the interference.... There is no requirement that the defendant intended to interfere with the personal property of another."[138] Therefore, even if the defendant accidentally or unintentionally interrupts the computer services of others, he or she may still be liable for the tort of trespass to chattels if their just "doing" the act was intentional.

{55} In the case of *United States v. Morris*[139] previously discussed, it could be argued that Morris may have been liable in tort under a theory of trespass to chattels to those persons whose computers his worm rendered unusable. Morris intentionally released his worm and knew it would occupy some computer operational time, thus depriving other users of their "property," however he just didn't realize how damaging

it would ultimately prove to be.[140]

{56} The second element of "intentional torts" that may be problematic to possible plaintiffs is damages. As previously discussed under the provisions of the Computer Fraud and Abuse Act, a plaintiff must suffer damages in excess of $5,000 before pursuing an action for an "interruption of computer service," however, quantifying those damages may be extremely difficult. The same is true in the context of trespass and intentional torts. "[A] prima facie claim[141] of trespass to chattels requires proof of actual damages."[142] Unfortunately, the type of damage that an authorized user might suffer at the hands of one who "interrupts" their service would mostly likely be "economic" in nature. Sidney R. Barrett, Jr. aptly defines the "economic loss" doctrine in his article, *Recovery of Economic Loss in Tort for Construction Defects: A Critical Analysis*[143] when he states, "[t]he economic loss doctrine marks the fundamental boundary between contract law, which is designed to enforce the expectancy interests of the parties, and tort law, which imposes a duty of reasonable care and thereby encourages citizens to avoid causing physical harm to others."[144] Simply stated, "the loss of an expectancy interest created by contract, often described as the 'benefit of the bargain,'" may not be recovered under a tort theory.[145]

{57} In the context of an interruption of one's computer service, economic losses would typically include lost operational time, forfeited business, possible damage or loss to information stored on disks and in memory, and costs of installing new security measures. There would probably be little actual "property" damage as a result of such an interruption. Contrary to mainstream jurisprudence which does not consider economic losses as property damage, a minority of jurisdictions do permit recovery of economic losses under various tort theories.[146] Even then, however, it is not assured that a lawsuit alleging such tortious conduct would be successful.

{58} On the other hand, some state legislatures have now begun drafting criminal statutes to recognize "property" rights in intangible computer data,[147] information and even computer time.[148] For instance, a New Hampshire statute reads, "Section 638:16 Computer Crime; Definitions. For the purpose of this subdivision: X. "Property" means anything of value, including data."[149] "The Supreme Court has also repeatedly recognized that information may be treated like property in such non-tort contexts as tax and due process."[150] All of this makes an action in tort more likely today than ever before.

ii. Tortious Interference

{59} Another possible cause of action in tort available to one who suffers an interruption of computer services arises out of applying contract law, and is called "tortious interference." This tort, which may be specifically referred to as a "tortious interference with contractual relations" or "tortious interference with prospective advantage," involves a defendant who causes a third party to breach an existing contract with the plaintiff.[151] For example, a perpetrator who intentionally incites America Online to break a service contract with one of its authorized users may be guilty of "tortious interference." In the context of an interruption of computer services, innocent users may sue offenders for interference with their contractual rights to unhampered computer usage furnished by computer service providers.[152] The elements essential to recovery for a tortious interference with a contract are: (1) the contract; (2) the wrongdoer's knowledge thereof; (3) his intentional procurement of its breach; (4) his actions are the proximate cause of the breach; and (5) damages resulting therefrom.[153] In other words, the plaintiff must demonstrate that the offender intended to interfere with the plaintiff's contractual relations, he (the offender) acted with knowledge that an interference would result, and he acted for an improper purpose.

{60} For example, in the case of *United States v. Morris,*[154] as previously discussed, if it had been Morris' intent to disrupt the computer services of authorized users by somehow interfering in the contractual obligation the service provider had to maintain service to those users, then a tortious interference would have occurred. In the case of *In re Brandl,*[155] a bookkeeper/computer operator allegedly programmed a

computer virus onto the software that the plaintiff maintained for the preservation and processing of his business records.[156] The plaintiff alleged that the operation of the virus caused damage to his business relationships with his customers, and resulted in a substantial loss of revenues.[157] The plaintiff brought his complaint under a theory of intentional interference with business relations and intentional interference with prospective business advantage.[158] The bookkeeper did not timely serve an answer to the plaintiff's complaint, so a default judgment was issued in favor of the plaintiff.[159] Thus, it is unclear whether the plaintiff would have succeeded in his tortious interference actions.

iii. Negligence

{61} Negligence is "the failure to exercise the standard of care that a reasonably prudent person would have exercised in a similar situation."[160] "The term refers to conduct which falls below the standard established by law for the protection of others against unreasonable risk."[161] The essential elements of negligence "are the existence of a legal duty owed by a defendant to a plaintiff, breach of that duty, and a causal relation between the defendant's conduct and the resulting damage to plaintiff."[162] In the context of the crime of an "interruption of computer services to authorized users," the perpetrator causing the interruption would have to owe some type of legal duty to the authorized computer user suffering the damage.

{62} For example, let's suppose that a user of America Online (AOL) in California somehow manages to disrupt the services of another AOL user in Maryland. For there to be evidence of a negligent act, it must be shown that the user in California owed some type of legal duty to the user in Maryland. Invariably, that situation would be difficult if not impossible to prove, thus such an action may not be available.

{63} In the above scenario, the user in California *would* invariably owe a legal duty to the provider of the service, in this case America Online, however, America Online might not have "standing"[163] to sue if they did not suffer any injuries as a result of the interruption to another user.

c. Other Statutory Actions

{64} Many states include a number of other provisions as part of their computer crime statutes which allow one who has been "injured" by an interruption of their computer services to pursue a variety of sanctioned remedies against the perpetrator of such activity. These actions may include temporary restraining orders, injunctions,[164] restitution for unjust riches garnished by the perpetrator in the commission of their crime, [165] treble damages in cases of malicious conduct, and restrictions on the offender's use of computers.[166] Typical of such a statute is Chapter 925, Section 52-570b of the Connecticut General Statutes Annotated. It reads as follows:

Section 52-570b. Action for computer-related offenses

> (a) Any aggrieved person who has reason to believe that any other person has been engaged, is engaged or is about to engage in an alleged violation of any provision of section 53a-251 [the section dealing with computer crime] may bring an action against such person and may apply to the superior court for:
>
> > (1) An order temporarily or permanently restraining and enjoining the commencement or continuance of such act or acts;
> >
> > (2) an order directing restitution; or
> >
> > (3) an order directing the appointment of a receiver.

* * *

> (c) Independent of or in conjunction with an action under subsection (a) of this section, 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. The aggrieved person shall recover actual damages and damages for unjust enrichment not taken into account in computing damages for actual loss, and treble damages where there has been a showing of willful and malicious conduct.[167]

B. *Comparison of State Laws*

{65} Forty-nine states now have enacted computer crime legislation.[168] These laws were legislated to "expand the degree of protection afforded to individuals, businesses, and government agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."[169]

{66} As initially discussed, although a number of states have statutes to ensnarl one who commits an interruption or denial of computer services,[170] many of those laws are not specifically addressed to authorized users. For instance, Texas Section 33.01, "Definitions," subsection (14) states that, "'Harm' includes partial or total alteration, damage, or erasure of stored data, *interruption of computer services*, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct."[171] Or, Maryland's Code Section 146, "Unauthorized access to computers prohibited," which states:

> (c) Illegal access. -- (2) A person may not intentionally, willfully, and without authorization access, attempt to access, cause access, or exceed the person's authorized access, to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to: (i) Cause the malfunction or *interrupt* the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services; . . . ."[172]

{67} Conceivably, one who interferes with the computer services of another would fall under the auspices of either of these laws; neither statute, however, specifically refers an interruption of access rights conferred upon authorized users. The following state statutes focus directly on this defined class.

State Statutes Focused on Interruption of Access Rights Conferred Upon Authorized Users

CALIFORNIA	**Section 502. Unauthorized access to computers, computer systems and computer data** (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense: (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.[173]

CONNECTICUT	**Section 53a-251. Computer crime** (a) Defined. A person commits computer crime when he violates any of the provisions of this section. (d) Interruption of computer services. A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.[174]
DELAWARE	**Section 934 Interruption of computer services.** A person is guilty of the computer crime of interruption of computer services when that person, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.[175]
FLORIDA	**Section 815.06. Offenses against computer users** (1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.[176] * * * The following three Florida news stories report some of the few instances of anyone ever being charged with the crime of an interruption or offense against another computer user: William Thomas Gossett, 18, of Weyford Lane, was charged with 23 counts each of offenses against computer users and fraudulent use of a credit card, according to a Pasco County Sheriff's Office report. Gossett [was] accused of stealing the ATM card and code of [an acquaintance]. Detectives said Gossett knew the access number because he had helped the acquaintance with an ATM transaction. He kept the card and continued using it at banks across the west side of the county. He stole a total of $2,780, the report stated. [177] LARGO - An 18-year-old man enrolled in college computer classes found himself [] jailed and accused of illegally tapping into the computer system of the Largo Diagnostic Clinic.

	Robert Christopher Gardner of Largo was charged with offenses against computer users. Gardner [was] accused of using the telephone modem on his home computer to gain access to the laboratory computer system at the medical clinic at 1551 W Bay Drive. "So many improper commands were sent to the computer that it trashed it," said Largo Det. Hank Klyse Jr. "For six hours, it was down. No one could access it...." He identified Gardner, who could not be reached for comment.[178] Two students at St. Petersburg Junior College were jailed [] on charges that they infiltrated a computer system that links libraries at 28 colleges in Florida. Police accused the students of creating a file, that bogged down a system operated by the Community College Center for Library Automation and interrupted transmission of electronic mail between the state's community colleges. "Jason Michael Levine, 19, of 13747 Martinique Drive in Seminole, and Cedric Rochefort, 18, of 12320 90th Ave. N. in Seminole, were held on $10,000 bail each" and charged with committing offenses against computer users and computer equipment: second and third-degree felonies.[179]
GEORGIA	**Section 16-9-93 Computer crimes defined; exclusivity of article; civil remedies; criminal penalties.** (a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; . . . shall be guilty of the crime of computer theft.[180] **Section 16-9-92 Definitions.** As used in this article, the term: (9) "Use" includes causing or attempting to cause: (B) The obstruction, interruption, malfunction, or denial of the use of a computer, computer network, computer program, or data; . . .[181]
ILLINOIS	**Section 5/16D-3. Computer tampering** S 16D-3. Computer Tampering. (a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:

	(4) Inserts 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 any other computer subsequently accessing or being accessed by 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 in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program".[182]
LOUISIANA	**Section 73.4. Offenses against computer users** A. An offense against computer users is the intentional denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network, or computer services.[183] * * * In a recent Louisiana story entitled, "E-mail Hacking Suspect Arrested,": > Louisiana State University (LSU) police arrested a thirty-year-old LSU student, suspected of hacking into another student's e-mail l account. [The] female student called the LSU Computer Services on November 6 and complained about problems with her school-sponsored e-mail, Captain Mark Shaw said.[184] An LSU systems analyst, who investigated the complaint, "found the account had been tampered with and called campus" police.[185] > After interviews, detectives learned that a classmate of the female student, Mr. Jean Michael Pepper, 30, was demanding that she 'do some things,' Shaw said, or he would forward some of her e-mail and cause her to lose her account. Shaw said he could not say exactly what Pepper demanded of the woman. Pepper was interviewed by detectives on November 12 and was given a misdemeanor summons for offenses against intellectual property and offenses against computer users," Shaw said.[186]
MISSISSIPPI	**Section 97-45-5. Offense against computer users; penalties.** (1) An offense against computer users is the intentional: (a) Denial to an authorized user, without consent, of the full and effective use of or access to a computer, a computer system, a computer network or computer services; . . .[187]
MISSOURI	**Section 569.099. Tampering with computer users, penalties** 1. A person commits the crime of tampering with computer users if he knowingly and without authorization or without reasonable grounds to believe that he has such authorization:

	(2) Denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, or on behalf of, or in conjunction with another.[188]
NEVADA	**Section 205.477 Unlawful interference with or denial of access or use; unlawful use.** 1. Except as otherwise provided in subsection 3, a person who knowingly, willfully and without authorization interferes with, denies or causes the denial of access to or the use of a computer, system or network to a person who has the duty and right to use it is guilty of a misdemeanor.[189]
NEW HAMPSHIRE	**Section 638:17 Computer Related Offenses.** III. A person is guilty of the computer crime of interruption of computer services when he, without authorization, knowingly or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.[190]
NORTH CAROLINA	**Section 14-456 Denial of computer services to an authorized user.** (a) Any person who willfully and without authorization denies or causes the denial of computer, computer system, or computer network services to an authorized user of the computer, computer system, or computer network services is guilty of a Class 1 misdemeanor.[191]
OHIO	**Section 2913.81 Denying Access To a Computer** (A) No person, without privilege to do so, shall knowingly deny or cause the denial of a computer system or computer services to an authorized user of a computer system or computer services that, in whole or in part, are owned by, under contract to, operated for, or operated in conjunction with another person.[192]
OKLAHOMA	**Section 1953. Prohibited acts** A. It shall be unlawful to: 6. Willfully and without authorization disrupt or cause the disruption of computer services or deny or cause the denial of access or other computer services to an authorized user of a computer, computer system or computer network.[193]
SOUTH CAROLINA	**Section 16-16-20. Offenses; penalties.** (3)(a) A person is guilty of computer crime in the second degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is greater than one thousand dollars but not more than twenty-five thousand dollars. (b) A person is also guilty of computer crime in the second degree where: (i) he interferes with, causes to be interfered with, denies or causes to be

	denied any computer service to an authorized user of the computer service for the purpose of devising or executing any scheme or artifice to defraud, or obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, or committing any other felony; . . . [194]
TENNESSEE	**Section 39-14-601 Definitions.** As used in this part, unless the context otherwise requires: (1) "Access" means to approach, instruct, communicate or connect with, store data in, retrieve or intercept data from, or otherwise make use of any resources of a computer, computer system or computer network, or information exchanged from any communication between computers or authorized computer users and electronic, electromagnetic, electrochemical, acoustic, mechanical or other means;[195] **Section 39-14-602 Violations -- Penalties.** (b) Whoever intentionally and without authorization, directly or indirectly: (1) Accesses any computer, computer system, or computer network commits a Class C misdemeanor; . . .[196]
VIRGINIA	**Section 18.2-152.2 Definitions.** For purposes of this article: "Property" shall include: 4. Computer services. A person "uses" a computer or computer network when he: 2. Attempts to cause or causes the withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; . . .[197] **Section 18.2-152.3 Computer fraud.** Any person who uses a computer or computer network without authority and with the intent to: 1. Obtain property or services by false pretenses; . . . shall be guilty of the crime of computer fraud.[198]
WEST VIRGINIA	**Section 61-3C-8 Disruption of computer services.** Any person who knowingly, willfully and without authorization, directly or indirectly, disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized recipient or user of such computer services, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail

	not more than one year, or both.[199]
WYOMING	**Section 6-3-50A. Crimes against computer users; penalties.** (a) A person commits a crime against computer users if he knowingly and without authorization: (ii) Denies computer system services to an authorized user of the computer system services which, in whole or part, are owned by, under contract to, or operated for, on behalf of, or in conjunction with another. [200]

IV. CONCLUSION

{68} The crime of an "interruption of computer services to authorized users" is a forgotten malfeasance---little used, rarely invoked, and virtually never prosecuted. It is the "little sister" of the more highly publicized, bolder and more "spectacular" crimes of computer trespass or data manipulation for which daring computer hackers are known to engage. In fact, the crime of "interruption of computer services to authorized users" could be just as effective a weapon against electronic criminals if it were simply given more prosecutorial attention.

{69} Many states have computer "interruption" laws on the books in various forms, however, these statutes appear to be vague in defining to whom they are designed to protect.[201] Even federal statutes make reference to crimes of "interruption" or "denial of computer services" without really defining the beneficiaries of such laws.[202] The obvious trend is that these laws will continue to undergo further refinement, and become more prevalent in computer jurisprudence as new avenues are created to prosecute the electronic criminals of the future.

ENDNOTES[**]

[*] Mr. Nemerofsky is a C.P.A. and hold a B.S. in Accounting from the University of Maryland; an M.B.A. in Information Systems Technology from George Washington University; a J.D. from Whittier Law School; and an LL.M. in Tax from the University of Florida, May 2000.

[**]. **NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?*, 6 RICH. J.L. & TECH. 23 (Spring 2000), *at* http://www.richmond.edu/jolt/v6i5/article2.html.

[1]. Different states call this same type of crime by various names: "Offenses against computer users"

(Florida & Louisiana), *See infra* notes 148, 156; "Computer tampering" (Illinois), *See infra* note 155; "Tampering with computer users" (Missouri), *See infra* note 161; "Denying access to a computer" (Ohio), *See infra* note 165.

[2]. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, *The National Information Infrastructure Protection Act of 1996: Legislative Analysis* (last modified June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>.

[3]. The Computer Emergency and Response Team Coordination Center ("CERT/CC") was formed by the Defense Advanced Research Projects Agency ("DARPA"), part of the U.S. Department of Defense in November 1988 to work with the Internet Community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. CERT/CC is now part of the Survivable Systems Initiative at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. *See* Carnegie Mellon Software Engineering Institute, *Cert Coordination Center* (last updated Feb. 10, 2000) <http://www.cert.org>.

[4]. Carnegie Mellon Software Engineering Institute, *CERT Coordination Center 1998 Annual Report (Summary)*(visited Feb. 11, 2000) <http://www.cert.org/annual_rpts/cert_rpt_98.html>.

[5]. *See id*.

[6]. "'Computer hacking' means accessing all or part of a computer, computer system, or a computer network for the purpose of establishing contact only without the intent to defraud or commit any other crime after such contact is established and without the use of computer-related services except such services as may be incidental to establishing contact," S.C. CODE ANN. § 16-16-10(j)(1998).

[7]. "A virus consists of a computer program designed to cause a diversion of resources, damage to data, or other permanent or temporary disruption in the operation of a computer system." Raymond T. Nimmer, The Law of Computer Technology, 64 § 12.22 (3rd ed. 1997).

[8]. *See generally* CAL. PENAL CODE § 502(10) (West 1998). "'Computer contaminant' means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self- replicating or self-propagating and 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, computer system, or computer network." *Id*. *See also* State v. Riley, 846 P.2d 1365, 1371 (Wash. 1993) (holding that defendant's hacking was sufficient evidence to convict him of two counts of computer trespass).

[9]. Approximately nineteen states appear to have laws specifically identifying the crime of an interruption or denial of computer services to authorized users. *See* discussion *infra*.

[10]. *See* Michael E. Ruane, *New Computer Technology Makes Hacking a Snap,* Wash. Post, March 10, 1999, at A1.

[11]. *See* 18 U.S.C. § 1030; nns. 170 et al., *infra*.

[12]. 704 A.2d 904 (Md. 1998).

[13]. *See id*. at 906.

[14]. *See id*.

[15]. *Id*.

[16]. *Id*.

[17]. *Id*. at 910 n.8.

[18]. *See DoS Attacks Information Page, Rapter mIRC Scripts Archive* (visited Feb. 12, 2000) <http://raptor.nu/dos.shtml>.

[19]. *See* John Barkley, *Denial of Service* (last modified Oct.7, 1994) <http://www-08.nist.gov/nistpubs/800-7/node117.html>.

[20]. *See DoS attack*, *PC Webopedia Definition and Links* (last modified Feb. 10, 1997) <http://webopedia.internet.com/TERMS/D/DoS_attack.html>.

[21]. *See* Sean Dugan, *Cybersabotage*, Infoworld (last modified May 19, 1998) <http://www.infoworld.com/cgi-bin/displayStory.pl?/features/97021cyber.htm>.

[22]. *See* Hans Husman, *Introduction to Denial of Service* (last modified Feb. 14,1997) <http://www.geocities.com:0080/TimesSquare/Dungeon/9058/hack.htm>.

[23]. *See* Dugan, *supra* note 20.

[24]. *See Denial-of-Service Incidents*, CERT Coordination Center Research (visited Feb. 14, 2000) <http://www.cert.org/research/JHThesis/Chapter11.html>.

[25]. *See* Barkley, *supra* note 18.

[26]. *See Denial-of-Service Incidents*, *supra* note 23.

[27]. *Denial of Service,* Association for Computing Machinery, University of Illinois, Urbana-Champaign (visited Feb. 14, 2000) <http://www.acm.uiuc.edu/workshops/security/deny.html>.

[28]. *DoS attack*, *supra* note 19.

[29]. *DoS Attacks Information Page*, *supra* note 17.

[30]. *See Denial of Service*, Java Security (last modified May 10, 1996) <http://java.sun.com/sfaq/denialOfService.html>.

[31]. *See Eugene E. Kashpureff Pleaded Guilty to Unleashing Software on the Internet*, The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice (last modified Mar. 19, 2000) <http://www.usdoj.gov/criminal/cybercrime/kashpurepr.htm>.

[32]. *See id*.

[33]. *See Juvenile Computer Hacker Cuts Off FAA Tower,* The Computer Crime and Intellectual Property Section of the (visited Feb. 14, 2000) <http:///www.usdoj.gov/criminal/cybercrime/juvenilepld.htm>.

[34]. *See id*.

[35]. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190 (1984)(codified as amended at 18 U.S.C. § 1030 (West 1998)).

[36]. Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem,* 43 VAND. L. REV. 453, 459-460 (1990).

[37]. *See id*. at 460.

[38]. *See id*.

[39]. Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986)(codified as amended at 18 U.S.C. § 1030 (a)(5) (West 1998)).

[40]. *Id*.

[41]. The term "Federal interest computer" means a computer--

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.

Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(e)(2)(A), (B) (1988).

[42]. 18 U.S.C. § 1030(a)(5) (1998).

[43]. *Id*.

[44]. *See id*.

[45]. As of this writing, there have been less than ten reported cases prosecuted under the Computer Fraud and Abuse Act.

[46]. 928 F.2d 504 (2d Cir. 1991), *cert. denied* 502 U.S. 817 (1991).

[47]. *See id*. at 505.

[48]. "[A] 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.' It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." United States v. Morris, 928 F.2d 504, 505 n.1. (2d Cir. 1991).

[49]. *See id*. at 505.

[50]. *Id*.

[51]. *Computer whiz guilty of planting rogue virus*, CHICAGO SUN-TIMES, Jan. 23, 1990, at 3, *available in* 1990 WL 4381438.

[52]. *Morris*, 928 F.2d at 505.

[53]. *Id*. at 506.

[54]. *See id*.

[55]. *Id*. at 506.

[56]. 18 U.S.C. § 1030 (a)(5)(A) (1986).

[57]. *See id*.

[58]. *Morris*, 928 F.2d at 507.

[59]. *See id*. at 509.

[60]. *Id*. at 508 (quoting S. Rep No 99-432, 99th Cong., 2d Sess. 5 (1986), reprinted in 1986 USCCAN 2479, 2484).

[61]. *Id*. at 505.

[62]. *See Morris*, 928 F.2d 504(2d Cir. 1991).

[63]. *See* Pub. L. No. 103-322, 108 Stat. 1796 (1994)(codified at 42 U.S.C. § 13701 (1994)).

[64]. *See id*.

[65]. "A person acts recklessly. . .when he consciously disregards a substantial and unjustifiable risk. . . [which as such] involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation." MODEL PENAL CODE § 2.02, U.L.A. (1997).

[66]. An intentional act is one in which "the actor desires to cause [the] consequences of his act, or that he believes that the consequences are substantially certain to result from it." BLACK'S LAW DICTIONARY, 810 (6th ed. 1990).

[67]. *See* 18 U.S.C. § 1030(a)(5) (1998).

[68]. *Id*.

[69]. *See id*.

[70]. *See id*. at (a)(5)(i)(II).

[71]. The following remarks were made by Senator Leahy of Vermont in the Senate on October 2, 1996:

> Every technological advance provides new opportunities for legitimate users and the potential for criminal exploitation. Existing criminal statutes provide a good framework for prosecuting most types of computer-related criminal conduct. But, as technology changes and high technology criminals devise new ways to use technology to commit offenses we have yet to anticipate, we must be ready to readjust and update our Criminal Code.

Hearings on S.982, Remarks of Sen. Leahy on the Economic Espionage Act of 19996, 104th Cong. (1996), available at <http://thomas.loc.gov/> (last visited Feb. 15, 2000).

[72]. *See id*.

[73]. *See* S. 982, 104th Cong.; 1st Sess. (1995).

[74]. Pub. L. No. 104-294, Title II, § 201, 110 Stat.3488, 3491-94 (codified at 18 U.S.C. § 1030 (1998)).

[75]. Pub. L. No. 104-294, Title I, § 101, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839 (1998)).

[76]. The term "protected computer" means a computer--

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication.

Computer Fraud and Abuse Act, 18 U.S.C. 1030 (e)(2)(A),(B)(1998).

[77]. *See* Pub. L. No. 104-294, Title II, § 210, 110 Stat. 3488 (1998).

[78]. 18 U.S.C. § 1030 (a)(5)(1998).

[79]. 928 F.2d 504, 509 (2d Cir. 1991), *cert. denied* 502 U.S. 817 (1991).

[80]. First offense negligent damage caused by a trespasser (i.e. unauthorized user) is a misdemeanor, while intentional or reckless damage caused by a trespasser (i.e. unauthorized user) is punished as a felony. 18 U.S.C. § 1030 (a)(5)(1998). *See* "Sentencing" discussion *infra*.

[81]. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, at 11 (last updated June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>.

[82]. 18 U.S.C. § 1030 (a)(5)(A)(i)(II) (1994).

[83]. 18 U.S.C. 1030 § 1030 (a)(5)(C)(1999). This language is similar to the wording of section (a)(5)(A)(i)(I) in the 1994 Act which stated that whoever knowingly intended to "damage, or cause damage to, a computer, computer system . . . ." 18 U.S.C. § 1030 (a)(5)(A)(i)(I)(1994).

[84]. *See supra* note 56.

[85]. *See* discussion *supra*.

[86]. America Online, Inc. v. LCGM, Inc., 45 F.Supp.2d 444, 446 (E.D.Va. 1998).

[87]. *Id*. at 450-451.

[88]. The 1994 Amendment to the 1986 Computer Fraud and Abuse Act amended subsection 1030 (a)(3) by inserting "adversely" before "affects" the use of the Government's operation of such computers. The language was modified once again by the 1996 Amendment which deleted the word "adversely" before "affects" because to include this term suggests, inappropriately, that trespassing in a government computer may be benign. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice (last updated June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime>.

[89]. 18 U.S.C. § 1030(a)(3)(1998).

[90]. Glenn D. Baker, *Trespassers Will be Prosecuted: Computer Crime in the* 1990's, 12 COMPUTER L.J. 68 (1993).

[91]. 18 U.S.C. § 1030 (1998).

[92]. *See* Pettingill v. Booth Newspapers, Inc., 278 N.W.2d 682, 684 (Mich. Ct. App. 1979)(holding that a newspaper publisher could not escape liability for actual damages caused by libelous matter published in a classified advertisement on grounds that the procedure for processing such ads was highly automated). One way for service providers to deflect potential liability from harmful viruses infiltrating their systems is to utilize disclaimers for their services and product. *See* Robin A. Brooks, Note, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*,17 REV. LITIG. 343, 391 n.194 (1998). By the same token, the user receiving the message may be contributorily negligent for failing to follow, at a minimum, reasonable practices for monitoring possible virus attacks through the use of virus detection software. *See id.* at 380.

[93]. 18 U.S.C. § 1030 (a)(5) (1998).

[94]. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, at 10 (last updated June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>.

[95]. Marc S. Friedman & Kristin Bissinger, Presented by Mary J. Hildebrand, *"Infojacking": Crimes on the Information Suprehighway*, 507 PLI/Pat 1107 *in* EIGHTEENTH ANNUAL INSTITUTE ON COMPUTER LAW (Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. G-507, 1998).

[96]. 928 F.2d 504 (2d Cir. 1991), *cert. denied* 502 U.S. 817 (1991).

[97]. *See id.* at 505.

[98]. *See id.* at 506.

[99]. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, at 9 (last modified June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime>.

[100]. 18 U.S.C. 1030 (a)(5) (1998).

[101]. Friedman and Bissinger, *supra* note 94, at 1114.

[102]. *See id.*

[103]. Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH., 699, 732 n.25 (1998).

[104]. *See supra* note 5.

[105]. Mitchell & Banker, *supra* note 102.

[106]. *See supra* note 38.

[107]. The doctrine of "de minimis non curat lex" means that "[t]he law does not concern itself with trifles." BLACK'S LAW DICTIONARY, 443 (7th ed. 1999).

[108]. 728 F. Supp. 1105 (D. Del. 1990).

[109]. *See id*. at 1106.

[110]. *See id*. at 1115.

[111]. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, at 11 (last modified June 10, 1998) <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>.

[112]. 18 U.S.C. § 1030(e)(8) (1998).

[113]. Computer Fraud and Abuse Act, Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1214 (1986)(codified as amended at 18 U.S.C. § 1030 (a)(5) (1998)).

[114]. *See* DOJ, *supra* note 89, at 3.

[115]. 18 U.S.C. § 1030(c)(1998).

[116]. *See* 18 U.S.C. Federal Sentencing Guidelines, § 2B1.3 (1998)(Historical Notes). Special instructions were added to § 2B1.3 of the Federal Sentencing Guidelines to provide that the minimum guideline sentence for those convicted under 18 U.S.C. § 1030(a)(5) was six months imprisonment. These provisions implemented a directive to the U.S. Sentencing Commission in section 805(c) of the Antiterrorism and Effective Death Penalty Act of 1996, Pub.L. 104-132, 110 Stat. 1305. The effective date of this amendment was November 1, 1997.

[117]. Under 18 U.S.C. § 1030 (a)(5) (1998), an authorized user of a protected computer who negligently or recklessly causes damage to another user as a result of improper access commits no crime; however, he is responsible for the cost of those damages.

[118]. Under the Federal Sentencing Guidelines, a violation of the Computer Fraud and Abuse Act (CFAA) section (a)(5) is considered "Property Damage or Destruction," which is located in "1. Theft, Embezzlement, Receipt of Stolen Property, and Property Destruction" (18 U.S.C., Federal Sentencing Guidelines, Ch. 2, Pt. B, § 2B1.3 (1998)) per Statutory Index. 18 U.S.C., Federal Sentencing Guidelines, App. A (1998). Also, under the Federal Sentencing Guidelines, a violation of section (a)(3) of the CFAA is considered a "Trespass," which is located in "2. Burglary and Trespass" (18 U.S.C., Federal Sentencing Guidelines, Ch. 2, Pt. B, § 2B2.3 (1998)) per Statutory Index. 18 U.S.C., Federal Sentencing Guidelines, App. A (1998). CFAA section (a)(3) is subject to the same offense level as section (a)(5). 18 U.S.C. Federal Sentencing Guidelines, Ch. 5, Pt. A (1998).

[119]. 18 U.S.C. § 3553 (1998).

[120]. *Id*.

[121]. Steven H. Gifis, LAW DICTIONARY, 320 (4th ed. 1996); *see also* BLACK'S LAW DICTIONARY, 633, 1014 (7th ed. 1999).

[122]. LA. REV. STAT. ANN. § 14:73.4 (1997).

[123]. NEV. REV. STAT. ANN. § 205.477 (1997).

[124]. *Compare* Nevada's misdemeanor punishment (*see supra* note 100) for one who "interferes" with computer services to Alaska's felony punishment for altering computer data. In Alaska, a person who knowingly accesses a computer and introduces false information with the intent to damage the data record of

a person may be convicted of a Class C felony. One convicted of a Class C offense may be sentenced to a definite term of imprisonment of not more than 5 years, and a fine of $50,000. ALASKA STAT. §§ 11.46.740, 12.55.125, 12.55.035 (Michie 1998).

[125]. A civil action is brought to enforce, redress or protect private rights, as opposed to a criminal action which pertains to the administration of the penal justice system. BLACK'S LAW DICTIONARY, 245 (6th ed. 1990).

[126]. 18 U.S.C. § 1030(g) (1998).

[127]. 928 F.2d 504 (2d Cir. 1991.

[128]. *See id*.

[129]. *See* GA. CODE ANN. § 16-9-93(g)(3)(1998) which states that, "[t]he provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law"; R.I. GEN. LAWS § 11-52-6 (1998), "[a]ny person injured as a result of this chapter [Chapter 52. Computer Crime] may bring a civil action against the violator for compensatory damages, punitive damages, court costs, and such other relief as the court deems appropriate, including reasonable attorneys' fees"; CAL. PENAL CODE § 502(e)(1)(West 1998), "In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."; TEX. CIV. PRAC. & REM. § 143.001 (West 1997), "[a] person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, [Computer Crimes] has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally."

[130]. 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 1998).

[131]. JOHN W. WADE ET AL., CASES AND MATERIALS, 1488-1489 (9th ed. 1994)

[132]. BLACK'S LAW DICTIONARY, 1489 (6th ed. 1990)

[133]. *See* Wade, *supra* note 109 at 1489.

[134]. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS, § 8, at 33 & n.5 (5th ed. 1988).

[135]. A trespass is the "unlawful interference with one's person, property, or rights." BLACK'S LAW DICTIONARY, 1502 (6th ed. 1990).

[136]. A "chattel" is a tangible and movable article of personal property as distinguished from real property. BLACK'S LAW DICTIONARY, 236 (6th ed. 1990). A trespass to chattels, therefore, is "[a]n unlawful and serious interference with the possessory rights of another to personal property." *Id.* at 1503.

[137]. W. PAGE KEETON ET AL., PROSSER AND KEETON ON LAW OF TORTS, § 14, at 85 & n.10 (5th ed. 1988).

[138]. *Id*. at 86 & n.13.

[139]. 928 F.2d 504 (2d Cir. 1991).

[140]. *See* discussion *supra*.

[141]. A prima facie case is one that is sufficient on its face, or on the first appearance. In Latin, it means "at first sight." BLACK'S LAW DICTIONARY, 1209 (7th ed. 1999).

[142]. *See* W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS, § 14, at 87 (5th ed. 1984) (stating "nominal damages will not be awarded . . . in the absence of any actual damage the action will not lie.").

[143]. Sidney R. Barrett, Jr., *Recovery of Economic Loss in Tort for Construction Defects: A Critical Analysis*, 40 S.C. L. REV. 891 (1989).

[144]. *Id*. at 894-95 n.9 (citing to Sacramento Reg'l Transit Dist. v. Grumman Flexible, 158 Cal. App. 3d 289, 204 Cal. Rptr. 736 (1984).

[145]. See *id*. at 895.

[146]. Casa Clara Condominium Ass'n, Inc. v. Charley Toppino and Sons, Inc., 620 So.2d 1244, 1246 n.2 (Fla. 1993).

[147]. *See generally* OHIO REV. CODE ANN. § 2901.01(A)(10)(a) (1999), "'Property' includes, but is not limited to, cable television service . . . computer software, computer data, financial instruments associated with computers, and other documents associated with computers, or copies of the documents, whether in machine or human readable form . . . "; CONN. GEN. STAT. ANN. § 53a-250(11)(1997), "'Property' means anything of value, including data."

[148]. Robin A. Brooks, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 REV. LITIG. 343, 383, 391 n.224 (1998) (citing United States v. Sampson, 6 Computer L. Serv. Rep. 879, 880 (N.D. Cal., 1978) (reasoning that "conversion" as used in the statute could include misuse or abuse of property, and that appropriation of computer time and capacity fit within the contours of "use").

[149]. N.H. REV. STAT. ANN. § 638:16 (Michie 1997).

[150]. Raymond T. Nimmer, *The Law of Computer Technology*, § 15.10 (3rd ed. 1997)(citing Newark Morning Ledger Co. v. United States, 507 U.S. 546 (1993)). In *Newark*, the Court held that an intangible asset, such as the future revenues from subscribers of a newspaper, may be valued as property for tax purposes, and thus be depreciated even though it reflects only an expectancy of continued patronage. Newark Morning Ledger Co. v. United States, 507 U.S. 546, 566 (1993).

[151]. *See* 45 AM. JUR. 2D Interference § 37 (1999).

[152]. *See* Lawrence F. Young, *Combating Unauthorized Internet Access*, 35 JURIMETRICS J., 257, 260 (1995).

[153]. *See* 45 AM. JUR. 2D *Interference* § 37 (1999). *See also* American Sur. Co. v. Schottenbauer, 257 F.2d 6 (8th Cir. 1958)(holding a workman's compensation insurer liable for inducing one of its clients, Wabasso Creamery, to discharge one of its employees on grounds that the employee's diseased finger allegedly increased his risk).

[154]. 928 F.2d 504 (2d Cir. 1991), *cert. denied*, 502 U.S.817 (1991).

[155]. 179 B.R. 620 (Bankr. D. Minn. 1995).

[156]. *See id*. at 622.

[157]. *See id*.

[158]. *See id*.

[159]. *See id*.

[160]. BLACK'S LAW DICTIONARY, 1056 (7th ed. 1999).

[161]. Steven H. Gifis, LAW DICTIONARY, 333 (4th ed. 1996). *See also* BLACK'S LAW DICTIONARY, 1056 (7th ed. 1999).

[162]. Gifis, *supra* note 136 at 516. *See also* BLACK'S LAW DICTIONARY, 1056 (7th ed. 1999).

[163]. "Standing" means that a plaintiff has a personal stake in the outcome of a dispute sufficient to obtain judicial resolution of that controversy. The concept focuses on whether the litigant is the proper party to fight the lawsuit, and requires the plaintiff to be injured or have been threatened with injury. In other words, no party is entitled to argue an action unless he himself is adversely affected by it. BLACK'S LAW DICTIONARY, 1413 (7th ed. 1999).

[164]. An "injunction" is a court order prohibiting someone from doing some act which he is threatening or attempting to commit, or restraining him in the continuance thereof. Generally, it is a preventive and protective remedy, aimed at future acts. BLACK'S LAW DICTIONARY, 784 (6th ed. 1990).

[165]. *See generally* N.H. REV. STAT. ANN. § 638:18(IV)(1999) ("[T]he court in addition to any sentence of imprisonment or other form of sentence authorized . . .may, in lieu of imposing a fine, sentence the defendant to pay an amount fixed by the court, not to exceed double the amount of the defendant's gain from the commission of such offense") (citations omitted).

[166]. *See* WIS. STAT. ANN. § 943.70(4)(1999), "Computer Use Restriction. In addition to the other penalties provided for violation of this section, a judge may place restrictions on the offender's use of computers."

[167]. CONN. GEN. STAT. ANN. § 52-570b(a), (c) (West 1999).

[168]. All states except Vermont.

[169]. CAL. PENAL CODE § 502(a) (West 2000).

[170]. *See* discussion *supra* text accompanying note 141.

[171]. TEXAS PENAL CODE ANN.§ 33.01 (West 1997) (emphasis added).

[172]. MD. ANN. CODE art. 27, § 146 (c)(2)(I) (1998) (emphasis added).

[173]. CAL. PENAL CODE § 502 (West 2000).

[174]. CONN. GEN. STAT. ANN. § 53a-251 (West 1999).

[175]. DEL. CODE ANN. tit. 11, § 934 (1999).

[176]. FLA. STAT. ANN. § 815.06 (West 1999).

[177]. *Woman is charged with conspiring to sell cocaine Series: POLICE*, ST. PETERSBERG TIMES, Nov. 23, 1991, at 3, *available in* 1991 WL 9181829.

[178]. Jane Meinhardt, *Student hacker stalled clinic computer, police say*, ST. PETERSBERG TIMES, May 28, 1988, at 1;1;1, *available in* 1988 WL 2582743.

[179]. *Pair Charged with Jamming 28 Colleges' Computers*, ST. PETERSBERG TIMES, Jan. 21, 1994, at 3B, *available in* 1994 WL 5318777.

[180]. GA. CODE ANN. § 16-9-93 (1998).

[181]. GA. CODE ANN. § 16-9-92 (1998).

[182]. 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 1998).

[183]. LA. REV. STAT. ANN. § 14:73.4 (West 1997).

[184]. *Police and Fire Briefs*, THE BATON ROUGE ADOVATE, Nov. 24, 1998, at 2B, *available in* 1998 WL 4920198.

[185]. *Id*.

[186]. *Id*.

[187]. MISS. CODE ANN. § 97-45-5 (1998).

[188]. MO. ANN. STAT. § 569.099 (West 1997).

[189]. NEV. REV. STAT. ANN. § 205.477 (Michie 1997)(amended 1999).

[190]. N.H. REV. STAT. ANN. § 638:17 (1997).

[191]. N.C. GEN. STAT. § 14-456 (1997).

[192]. OHIO REV. CODE ANN. § 2913.81 (Baldwin 1998)(repealed 1996).

[193]. OKLA. STAT. ANN. tit. 21, § 1953 (West 1998).

[194]. S.C. CODE ANN. § 16-16-20 (Law Co-op. 1998).

[195]. TENN. CODE ANN. § 39-14-601 (1998).

[196]. TENN. CODE ANN. § 39-14-602 (1998).

[197]. VA. CODE ANN. § 18.2-152.2 (Michie 1998).

[198]. VA. CODE ANN. § 18.2-152.3 (Michie 1998).

[199]. W. VA. CODE § 61-3C-8 (1998).

[200]. WYO. STAT. ANN. § 6-3-504 (Michie 1998).

[201]. *See* discussion *supra*.

[202]. *See* 18 U.S.C. § 1030 (1998).
