Volume 6, Spring Issue, 1993

COMPUTER NETWORK ABUSE

*Michael P. Dierks**

INTRODUCTION

One may initially think that the development of legal boundaries in the binary world of electronic computing should be easy. One may envision a certain set of zeros and ones falling on the side of legality and a complementary set falling on the side of illegality. But such a vision is flawed. Although the microelectronic world of "cyberspace"[1] is premised on boundaries that are black and white, laws do not develop along such boundaries. Laws govern people, not places.[2] Moreover, laws are created by people, not algorithms. The mere fact that people act in cyberspace does not make their actions less human, nor does it shield actors from responsibility for their actions. To suggest that a person is not culpable for theft conducted through an illicit computer transfer is to suggest that a person is not culpable for murder committed by a hand-

---

* B.S.E., 1990, Duke University; J.D., 1993, Harvard Law School. Mr. Dierks will be an associate with the law firm of Weil, Gotshal & Manges in New York City in the fall of 1993.

1. The term "cyberspace" was first used by science fiction novelist William Gibson to describe the fantasy electronic world inhabited by the characters in his 1984 novel *Neuromancer*. In this fictional world of cyberspace, "computer cowboys" neurologically patch themselves into computer networks where matrices of electronic data become cerebral manifestations. Without keyboards or mice, the cowboys navigate their ways through data of individuals, firms, and governments as if the cowboys are suspended in a surreal fourth dimension.

As technology advances make some of the concepts of cyberspace less fictional, the term has been adopted to describe real-world electronic computer networks. Although current users do not physically patch themselves into networks, real-world networks are devoid of the time and space contraints that plague other aspects of daily life. Significantly, even the legal community has recognized this principle and has used the term cyberspace approvingly. *See, e.g.*, Laurence H. Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, Keynote Address at the First Conference on Computers, Freedom & Privacy (Mar. 26, 1991) (transcript available from Harvard Law School); Mitchell Kapor, *Civil Liberties in Cyberspace*, SCI. AM., Sept. 1991, at 158; Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 U. MO.-KAN. CITY L. REV. 139 (1991).

In this Article, the term "cyberspace" is used in its real-world sense. The term serves as a helpful surrogate for describing the electronic glue of wires, fiber-optic cables, telephones, switching-stations, satellites, and receiving-stations that comprise the thousands of small and large, national and international electronic computer networks.

2. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (finding that "the Fourth Amendment protects people, not places"); *see generally* Tribe, *supra* note 1, at 19, 22 (arguing that the Constitution, as a whole, should be read as protecting "people, not places").

gun.[3]

Cyberspace is a new forum, and the regulation of cyberspace presents novel legal issues. In addressing these issues, there are two basic approaches: rethinking old law, or creating new law.[4] On the one hand, present law could be applied to the regulation of cyberspace. This new forum may fit existing legal doctrine in such a perfectly symbiotic way that only a few statutory amendments and rational precedents are needed to reconcile it with existing law. On the other hand, fitting cyberspace into existing law may present the problem of fitting the square peg into the round hole. The cyberspace world may have underlying assumptions so different from the world in which traditional rights and responsibilities are conceptualized that such rights and responsibilities must themselves be rethought. But through this deconstruction, one may even discover that the square hole has been ignored.

This Article focuses on computer abuse in cyberspace: the unauthorized viewing, alteration, and misappropriation of data on networked computer systems.[5] To date, the only openly-stated method used to address this problem has been the criminal law, and commentators on the topic have suggested ways in which present computer crime law should be amended to face the alleged problem more effectively.[6] But, because

---

3. *See* 132 CONG. REC. H3275-04 (daily ed. June 3, 1986) (statement of Rep. Nelson that "[c]omputers may not commit crimes—any more than guns commit crimes").

4. *Cf.* Parker v. Flook, 437 U.S. 584, 595 (1978) (holding that a computer-based mathematical algorithm is not subject to patent protection and noting that "[t]o a large extent [such a] conclusion is based on reasoning derived from opinions written before the modern business of developing programs for computers was conceived"). In general, the debate over intellectual property rights in computer software represents a good example of the old law versus new law dichotomy in a technological context. Some commentators favor the application of existing copyright (or patent) law, but other commentators favor the adoption of a new, sui generis scheme of protection for computer software. *Compare* Anthony L. Clapes, Patrick Lynch & Mark R. Steinberg, *Silicon Epics and Binary Bards: Determining the Proper Scope of Copyright Protection for Computer Programs*, 34 UCLA L. REV. 1493 (1987) *and* Duncan M. Davidson, *Common Law, Uncommon Software*, 47 U. PITT. L. REV. 1037 (1986) (arguing for copyright protection) *with* John C. Phillips, Note, *Sui Generis Intellectual Property Protection for Computer Software*, 60 GEO. WASH. L. REV. 997 (1992) *and* Pamela Samuelson, *Applying the Lessons of the Chip Law to Computer Programs*, 70 MINN. L. REV. 471 (1985) (arguing for sui generis protection).

5. This definition of "computer abuse" applies throughout this Article. Other sources define this concept more broadly. The Department of Justice, for example, defines "computer crime" as "any illegal act for which knowledge of computer technology is essential for successful prosecution." OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: MANAGEMENT, SECURITY, AND CONGRESSIONAL OVERSIGHT 86 (1986). Such a definition, however, fails to distinguish between the theft of computer disks and the theft of computer data; it fails to isolate correctly the novel problems of criminal law raised by advanced technology.

6. Most commentators suggest expansion of present criminal liability as the solution to

the unique qualities of cyberspace challenge core principles of criminal law, these commentators have incorrectly attempted to force the world of cyberspace (the square peg) into the criminal law model of illegality (the round hole). In contrast to popular belief, present computer crime laws are already adequate in scope to prosecute all forms of computer abuse in almost any combination of jurisdictions.

Rather than viewing criminalization as the *sole* means of addressing the problem of computer abuse, ex ante measures to prevent computer abuse should be recognized for their more effective deterrent value. In other words, schemes for preventing computer abuse provide the illusive square hole that properly fit the square peg of cyberspace. A variety of legislative plans could be implemented to focus on prevention instead of criminalization. But in the end, such legislative schemes are unnecessary. Unless there is market failure in the market for computer security equipment, an efficient level of spending occurs on preventive measures with a corresponding efficient level of computer abuse. The invisible hand of the market correctly resolves the problem of computer abuse, and the ex post criminalization of computer abuse serves merely as a symbolic gesture of government's intolerance towards the problem, as well as a safety net for the prosecution of discovered offenders.

I. COMPUTER ABUSE: THE ALLEGED PROBLEM

This Section examines computer abuse and its portrayal in the media. It is divided into three Subsections. The first Subsection discusses computer crime and computer security. It looks at methods of ensuring

---

the alleged computer abuse problem. *See, e.g.*, Michael T. Friedman, Comment, *The Misuse of Electronically Transferred Confidential Information in Interstate Commerce: How Well Do Our Present Laws Address the Issue?*, 4 SOFTWARE L.J. 529 (1991) (arguing for clarification of existing federal law in prohibiting the "misuse of electronically transferred confidential information"); Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453 (1990) (arguing for adoption of federal computer security requirements and federal computer abuse reporting requirements and for creation of federal civil remedy for computer fraud); Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER/L.J. 265 (1991) (arguing for adoption of a uniform federal computer crime statute to guide federal law, as well as to serve as a model for state law). One commentator, though, suggests that present computer crime law is overbroad and fails to serve the goals of criminal law. *See* Brenda Nelson, Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299 (1991).

that access to a computer system is authorized, and it examines the costs and benefits of these methods. Based on this foundation, the second Subsection examines three specific media portrayals of computer criminals. It discusses the crimes committed by these notorious computer hackers,[7] and it analyzes the polar approaches to computer abuse adopted by these three criminals. The third Subsection examines the media portrayal of computer abuse. It argues that the media quantitatively overstates and qualitatively misstates the problem of computer abuse.

A. Computer Crime and Computer Security

Remote[8] use of computer systems is important for business, government, and academia. It allows users at physically distant locations to access the power, resources, and speed of systems otherwise unavailable to them. The LEXIS and Westlaw legal databases provide salient examples of the benefits of remote computing. The power to search entire bodies of law quickly for a particular phrase, issue, or idea is valuable to a lawyer. But, because of limitations of present technology

---

7. The term "computer hacker" is now synonymous with computer criminal and carries strong negative connotations. The origins of the term, however, are different. In the early days of computing at the Massachusetts Institute of Technology, the term "hack" was used by members of the model railroad club to refer to "a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement." STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 23 (1984). The title "hacker" was a badge of distinction for talented members of the model railroad club. As many of the members of the club defected to work on the then-new digital computers at MIT, the terms "hack" and "hacker" were adopted in the computing context. *See id.* at 23-24.

In this Article, the term "hacker" refers to a computer user who intends to gain unauthorized access to a computer system. Because the mere process of unauthorized entry is the focal point, the (criminal or other) intent of such a user is not important to the present definition. Moreover, the lack of criminal intent does not necessarily mean that a particular unauthorized entry will not result in serious economic or other injury. *Cf.* United States v. Morris, 928 F.2d 504, 509 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991) (rejecting defendant's argument that he lacked criminal intent to violate computer crime provisions of federal law).

8. The convention distinguishing between "remote" and "local" users adopted in this Article can also be thought of in terms of "off-site" and "on-site" users. While a remote, or off-site, user generally uses a modem and telephone connection to gain access to a particular computer system, a local, or on-site, user generally has a direct connection to the system. This distinction between remote and local users, however, is not relevant in distinguishing between degrees of criminal or fraudulent conduct. The remote or local nature of a user, though, does dictate which types of computer security measures are practical, see *infra* notes 13-14 and accompanying text. Moreover, the fact that a user is remote and out-of-state from the accessed computer implicates problems of jurisdictional bounds. *See infra* notes 92-93 and accompanying text.

and resulting economies of scale, individual lawyers cannot maintain their own detailed legal databases. In contrast, a collective database is a viable alternative. By allowing many users to share the costs of maintaining an extensive legal database, remote computing makes available an otherwise untenable resource.

But with this advantage of remote computing comes the concurrent problem of authenticating user identity. The form of user authentication most frequently used is the password,[9] a sequence of characters that one must enter prior to gaining access to a computer. Generally, individual users have their own unique passwords, and on many computer systems, individual users also have the ability to change their passwords at any time.

Unfortunately, password protection is often inadequate to prevent unauthorized access to a computer system. Particularly where passwords are based on dictionary words rather than sequences of random characters, it is not challenging for a hacker to gain unauthorized access to a computer.[10] The process is simple. The computer hacker instructs his or her computer to call the target computer and scroll through passwords until a valid one is discovered. Even if the target computer disconnects the hacker's computer after a predetermined number of unsuccessful password attempts, it is not difficult to program the hacker's computer to automatically reestablish its telephone connection with the target computer and continue the password scrolling process.

In addition to problems of remote authentication, the use of passwords for local authentication is problematic. It is not difficult for a first local user to steal the password of a second local user with greater computer access privileges than the first user. Computer users often affix their passwords to the computers themselves,[11] making theft of such passwords extremely simple. Additionally, "shoulder-surfing" is a common and

---

9. *See* Ann Sussman, *Variety of Methods Are Best When Plugging Security Holes*, PC WK., July 21, 1987, at 109.

10. *See id.*; Stephen T. Irwin, *What Corporate Users Should Know About Data Network Security*, TELECOMM., May 1991, at 49. The use of a dictionary word is particularly problematic. For example, on a hypothetical computer system using an eight character password, the fortuitous discovery of a valid password is more than 28,000,000 times as likely if passwords are based on a dictionary of 100,000 words than if passwords are based on random sequences of letters and numbers. Additionally, the threat of unauthorized access to an unencrypted (or poorly encrypted) password file presents a serious security problem, regardless of whether dictionary word or random passwords are used.

11. *See* Irwin, *supra* note 10.

simple method of stealing the passwords of fellow users.[12] Because local users also have greater knowledge of the intrinsic structural organization of their user groups, they know which users have particularly extensive computer privileges. Thus, knowledgeable local users pose a potentially greater threat to the overall security of a computer system than do remote users.

To patch the security holes inherent in a password-based system of user authentication, a number of more rigorous methods of user authentication are available.[13] For example, both encryption techniques and call-back systems decrease the possibility of remote computer abuse. By encrypting data sent over telephone lines, only remote users possessing the appropriate decryption software have access to the data. In call-back systems, the target computer calls the remote user at a predetermined telephone number. Thus, only remote users located at their correct remote telephone addresses have access to the target computer. A multitude of techniques are available to decrease the potential for local computer abuse, including biometric or mechanical systems of user authentication. In a biometric system, the local user is verified by a unique biological trait, such as voice or fingerprint. In mechanical systems of user authentication, the local user is verified by inserting a physical item into the computer terminal, such as a magnetic card or token. But, although these security systems increase the reliability of user authentication, they are expensive, and thus economically inefficient for many computer users.[14]

In addition to its high cost, the use of sophisticated security measures has an indeterminate affect on personal privacy. On the one hand, sophisticated computer security decreases user privacy. Because such systems are premised on ensuring that a user seeking access is a valid user, computer systems often must contain an increased amount of personal data, such as a user's social security number, home telephone number, fingerprint, or voiceprint. Of the methods of authentication discussed above, only encryption techniques and mechanical systems of authentication offer no infringement of personal privacy.

---

12. Sussman, *supra* note 9.

13. *See id.*; Ira W. Cotton, *Overcoming an Insecurity Complex—Magnetic Stripe Cards Could Help Solve the Computer Security Problem*, INFO. WK., Nov. 25, 1991, at 72; Irwin, *supra* note 10.

14. Biometric systems, for example, cost on the average $5000 per device. *See* Sussman, *supra* note 9.

On the other hand, the maintenance of such personal data on a computer system is a relatively minor infringement of personal privacy, and may even be irrelevant to some user groups. In any event, this infringement of personal privacy must be weighed against the relative gains in personal privacy resulting from the use of sophisticated computer security measures. There are at least two positive privacy effects. First, by decreasing the overall frequency of unauthorized access, legitimate users are subject to fewer invasions of privacy by private actors gaining access to sensitive or otherwise private data. Second, by addressing the problem of computer abuse from an ex ante perspective (i.e., preventing it) instead of from an ex post perspective (i.e., criminalizing it), legitimate users are also subject to fewer invasions of privacy in the form of overbroad criminal searches by public actors in investigations of particular crimes.

Even if cost and privacy issues did not pose barriers to increased computer security, such security measures would not prevent legitimate users from abusing their valid computer privileges.[15] This problem, though, is outside the scope of computer fraud because the acts of legitimate users are, by definition, "authorized" acts from the perspective of the computer.[16] Moreover, there is no need to consider these acts

---

15. *See* Belden Menkus, *"Crime Prevention" in System Design*, J. SYS. MGMT., May 1991, at 19. One flagrant case of insider abuse involved Robert Venezia. He allegedly embezzled at least $6.2 million from the First Fidelity Bank of Newark, New Jersey, by routinely using his *legitimate* power to authorize electronic payments. Over an 11 year period, he allegedly used this power to divert the $6.2 million sum to two shell corporations he created for the express purpose of receiving such illicit funds. *See id.*

16. *See supra* note 5 and accompanying text (defining "computer abuse" as the commision of "unauthorized" acts); *see also infra* notes 72-79 and accompanying text (noting that the Computer Fraud and Abuse Act of 1986 criminalizes the "unauthorized access" of a computer for certain illicit uses). Although this distinction might first strike the reader as semantic, a real distinction is present. For example, the misappropriation of bank funds by an employee with discretion over such funds differs from a bank robbery committed by a non-employee third party. The introduction of a computer to further either scheme should not change the character of the underlying acts.

The unique quality of electronic computer networks is their ability (or at least their attempt) to differentiate between legitimate users and illegitimate users. This unique quality should differentiate ordinary crime from computer crime, and a central element of computer abuse should be that the abusive user passes himself or herself off as a legitimate user. Thus, the bank employee exercising authorized discretion (i.e., the bank employee with extensive computer privileges) does *not* commit computer abuse; the third party exercising unauthorized discretion (i.e., the third party who convinces the computer that the third party is the bank employee with valid computer privileges) commits computer abuse. In the first instance, the fraud is commited on the employment relationship, the fraud is computer independent, and the act should not be punished as computer abuse. In the second instance, the fraud is commited on the computer system itself, the computer system is a necessary link in the commission of the fraud, and the act should be punished as computer abuse.

within the realm of computer fraud. From an ex post perspective, these acts are prosecutable under state law principles of agency and embezzlement,[17] and neither require nor suggest the use of criminal sanctions grounded in special theories of computer fraud. From an ex ante perspective, the most appropriate method of dealing with the problem is through management foresight. Businesses should adhere to policies that keep any single person from a position of absolute power. With a sufficiently balanced power structure, it becomes difficult for a single employee to abuse his or her legitimate computer privileges.

In summary, computer security is an important element in preventing computer abuse. While leaving one's house unlocked is not an invitation to steal its contents, it makes a burglar's job much easier. Similarly, limiting the availability of the "keys" to computer systems to those users with proper authority and responsibility to use a particular system is crucial. But responsibility within any organizational structure creates the opportunity for abuse, whether or not a computer system is an element in a scheme to defraud. The delegation of responsibility and the ability to hold a position of power and trust are human issues. Although increasing computer security reduces the potential for computer abuse, even the most secure computer systems are still subject to the problem of human greed.

B. Computer Abuse in the Media

The media portrays a world in which hackers sit nightly in front of personal computers and generate chaos in the computer systems of the United States and beyond.[18] For example, Kevin Mitnick caused $4

---

17. The definition of "embezzlement" is instructive in showing that abusive acts committed by legitimate users should not fall within the realm of computer abuse.

> To "embezzle" means willfully to take, or convert to one's own use, another's money or property, of which the wrongdoer acquired possession lawfully, by reason of some office or employment or position of trust. The elements of "offense" are that there must be a relationship such as that of employment or agency between the owner of the money and the defendant, the money alleged to have been embezzled must have come into the possession of defendant by virtue of that relationship and there must be an intentional and fraudulent appropriation or conversion of the money.

BLACK'S LAW DICTIONARY 522 (6th ed. 1990).

18. *See generally* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 105-07 (1988).

million in damage to computer giant Digital Equipment Corporation in Massachusetts without ever leaving the Los Angeles area.[19] Hans Heinrich Hubner, a West German computer hacker, stole computer software from western computers and sold it to the KGB prior to Germany's reunification.[20] And Robert Morris, a former computer science graduate student, single-handedly crashed the Internet computer network, which connects industry, government, and academia in the United States.[21] But as discussed in this Subsection, Mitnick and Hubner were not computer geniuses, and Morris, albeit a computer genius, crashed the Internet due to a mistake.[22] In broader terms, case studies of these three hackers shows that there are many "human" hackers, like Mitnick and Hubner, but few "computer" hackers like Morris.

1. Kevin Mitnick

To be sure, Mitnick pioneered some interesting tricks that made him a difficult criminal to snare. For example, he devised a method of avoiding telephone tracing through the use of the call-forwarding service of the telephone company.[23] An attempted trace to his telephone line would send the trace not to his own phone, but to one of his choosing. On one occasion, he also escaped arrest by knowing of the arrest warrant

---

19. *See, e.g.*, Kathy Barks Hoffman, *Addicted Hacker Gets Prison, Rehabilitation*, USA TODAY, July 19, 1989, at B2; John Johnson, *Computer as an "Umbilical Cord to His Soul": "Dark Side" Hacker Seen as "Electronic Terrorist,"* L.A. TIMES, Jan. 8, 1989, at A1.

20. *See, e.g.*, Robert J. McCartney, *Computer Hackers Face Spy Charges; West Germany Indicts 3 Accused of Selling Data to Soviet KGB Agent*, WASH. POST, Aug. 17, 1989, at A32; *Saturday Night with Connie Chung* (CBS television broadcast, Dec. 16, 1989).

21. *See, e.g.*, Carrie Gottlieb, *What to do About Computer Viruses*, FORTUNE, Dec. 5, 1988, at 16; John Markoff, *Author of Computer 'Virus' is Son of N.S.A. Expert on Data Security*, N.Y. TIMES, Nov. 5, 1988, at A1.

22. Case studies of these three hackers are presented in KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER (1991) [hereinafter CYBERPUNK]. This book deflates the image of the computer hacker created by the popular media.

> Hacking has achieved a glamorous reputation in recent years. Although most of the nerds who break unbidden into other people's computers have more in common with Pee Wee Herman than James Bond, they have nonetheless gained a reputation as a cross between 007 and Einstein. This reputation is entirely bogus. [*Cyberpunk*] debunks it.

Computer Hacking: Human Error, ECONOMIST, Sept. 14, 1991, at 106 (reviewing CYBERPUNK).

23. *See* CYBERPUNK, *supra* note 22, at 126.

and leaving the state before he could be apprehended.[24] These talents, though, are distinct from computer adroitness. Intimate knowledge of the phone system differs from the ability to access computers without authorization. Moreover, his knowledge of the arrest warrant was obtained by non-technical means. Impersonating a Los Angeles police officer, he learned of the warrant from a computer operator, not from the computer itself.[25]

Like most computer hackers, Mitnick's success in accessing computers without authorization directly related to his ability to obtain passwords illicitly. Because Kevin Mitnick possessed the social engineering skills to charm system users out of system passwords, he became a successful computer criminal.[26] To the extent that computer hackers such as Mitnick can find human ways of circumventing computer security, such systems are susceptible to computer abuse. Ofte he weakest element in many computer systems is the human element."[27]

2. *Hans Heinrich Hubner*

Like Mitnick, Hans Heinrich Hubner was essentially a human hacker, obtaining illicit passwords through friends and underground computer bulletin boards. In addition to this human quality of Hubner's computer

---

24. *See id.* at 76.

25. *See id.* at 76-77.

26. *See id.* at 64-65. Once Mitnick accessed a computer system, though, he did possess the technical expertise to ensure future system access. But his ability was attributable primarily to a technique developed by the Chaos Club, a West German computer hacker group. This group developed a method called the "login patch" to exploit an error in the operating system software used on computers made by the Digital Equipment Corporation. Without going into the details, the program let a user find out the passwords of other users. *See id.* at 113-15.

27. One computer abuser described the problem as follows:

> Take a computer and put it in a bank vault with ten-foot-thick walls. Power it up with an independent source, with a second independent source for backup. Install a combination lock on the door, along with an electronic beam security system. Give one person access to the vault. Then give one more person access to the system and the security is cut in half. With a second person in the picture . . . [one] could play the two against each other. She could call posing as the secretary of one person, or as a technician in for repair at the request of the other. She could conjure dozens of ruses for using one set of human foibles against another. And the more people with access the better. In the military, hundreds of people have access. At corporations, thousands do.

Id. at 61.

exploits, it is interesting to note how the media overstated the value of Hubner's computer thefts. Although the media portrayed Hubner as stealing and selling important national secrets,[28] the reality was much less interesting. On one occasion, Hubner's espionage group sold a program worth only 120 DM to the KGB agent for 4000 DM. On a separate occasion, they sold the KGB agent a variety of public domain programs—programs that are expressly intended for free distribution among computer users—for 2000 DM.[29] In the end, even the German authorities concluded that nothing of substance was sold to the KGB agent,[30] but such after-the-fact realizations seldom make headline news.

3. Robert Morris

As with Hubner, the media wildly overestimated the damage done by the computer "worm" created by Morris. The *Los Angeles Times*, for example, reported that the damage exceeded $97 million.[31] But as determined in federal district court, the actual damage amounted to only $150,000, with individual sites suffering damage of $200 to $53,000.[32] While this actual loss is not trivial, it nevertheless is insignificant in comparison to the $97 million estimate propagated by the popular press.

But unlike either Mitnick or Hubner, Morris possessed a high level of computer expertise. Of the "hacks" committed by these three, only the Morris worm is interesting from a computer science perspective.[33] The computer exploits of Mitnick and Hubner are based on human persistence and social engineering ability. Morris, on the other hand, created a unique method of gaining unauthorized access to computer systems. Precisely because the worm was novel and not based on human qualities, it was effective. In fact, the worm was so effective that it brought the entire Internet to its knees, crashing over 6000 computers during the night

---

28. *See* McCartney, *supra* note 20; *Saturday Night with Connie Chung*, *supra* note 20.
29. *See* CYBERPUNK, *supra* note 22, at 197.
30. *See id.* at 249.
31. *Damage From Computer Virus Set at $97 Million*, L.A. TIMES, Nov. 18, 1988, § 4, at 4 (quoting an expert as saying his estimate of $97 million was "very conservative [and that] the real cost is probably well over $100 million").
32. *See* United States v. Morris, 928 F.2d 504, 506 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991); *see also* CYBERPUNK, *supra* note 22, at 334.
33. The Morris worm received considerable technical discussion in the computer science literature. *See, e.g.*, Jon A. Rochlis & Mark W. Eichin, *With Microscope and Tweezers: The Worm From MIT's Perspective*, 32 COMM. ACM 689 (1989); *see also infra* note 38.

of November 2, 1988.[34] Neither Mitnick nor Hubner could achieve this level of computer chaos.

Morris had benign intentions. His goal was to find out how many computers he could access across the nation. He did not want to view, alter, or steal data from these other computers; he merely wanted to gain access to other systems without hurting other users.[35] The worm he created worked by exploiting certain holes in the UNIX operating system used on the Internet. Because sophisticated operating systems like UNIX must deal with many issues (e.g., multiple users, system security, and time sharing), these programs are large, diverse, and error-laden. Morris was fascinated with these errors in UNIX,[36] and he eventually became an expert in these security flaws.[37] Thus, it seemed natural for him to exploit the security holes he had discovered in UNIX to realize his goal of gaining unauthorized access to as many computer systems as possible.

It is unnecessary to explore the further details of the Morris worm.[38]

---

34. *See* sources cited in note 21.

35. *See* CYBERPUNK, *supra* note 22, at 295-99.

36. As an undergraduate at Harvard University, Morris spent hours reading the UNIX documentation that most users, even sophisticated ones, consult only as a reference. *See id.* at 285.

37. During the spring break of his senior year in college, he delivered a lecture on the topic to the National Security Association. *See id.* at 292.

38. For those readers interested in the details, the Morris worm worked as follows. It was a small, self-replicating program that exploited two errors in UNIX. The first error allowed a program on a first computer to be copied to a second computer; the second error allowed this copied program to be executed on the second computer without the need for user authorization. The worm used these errors to propagate from a first computer to a second computer. Once inside the second computer, the worm would determine which computers were networked to the second computer and then send itself to these other computers, perhaps the third through fifth computers. These third through fifth computers would repeat the process and send the worm to the perhaps sixth through hundredth computers. The process would continue *ad infinitum* until every computer on the Internet had at least one copy of the worm running on it. *See id.* at 295-99; *see also* Rochlis & Eichin, *supra* note 33.

Many computers, however, are connected to identical computers. For example, the sixth computer should know not to send the worm back to the third computer from whence it originated. If the worm did not limit its replication, every computer in the network would crash due to the infinite copying process. But the possibility that the worm could be stopped by a computer falsely indicating that it had a present copy of the worm created the threat of stopping the progression of the worm. Thus, Morris included a provision in the worm to replicate once in every seven times on computers indicating an existing copy of the worm. The problem was that the use of the one-in-seven ratio fell short of a realistic rate of replication by a magnitude of many thousands. Because the worm propagated so quickly throughout the Internet and because the rate of replication on previously infected computers was so high, the resources on many Internet computers became devoted to running thousands of copies of the worm. These computers crashed through the night before system managers even knew of the worm's existence.

The important consequence is that it crashed the Internet, bringing over 6000 computers to a grinding halt. Although this effect resulted from numerical miscalculation on the part of Morris, the worm showed the vulnerability of computer networks. Moreover, someone with Morris's knowledge of UNIX and a less benign intent could have produced far greater damage. The Morris worm indicated that even the most theoretically secure computers are still susceptible to computer abuse by knowledgeable computer users.

4. Analysis

While Mitnick, Hubner, and Morris all received significant negative press, the worm unleashed by Morris stands as the only interesting "computer" abuse to date. Mitnick and Hubner achieved notoriety by capitalizing on human weaknesses. They were con-men with computers instead of cards. Mitnick exploited the human element of trust. By falsely acquiring the trust of important system users, he was able to acquire an impressive repertoire of passwords. Hubner exploited computer ignorance; he sold lead to the KGB agent expecting gold. Only Morris showed that computers themselves could be used in the process of computer abuse as more than a mere surrogate for human cunning.

C. The Fallacies in the Media Portrayal of Computer Abuse

1. Quantitative Overstatement

On an aggregate level, computer abuse results in smaller quantitative losses than the media portrays. Although the losses due to computer abuse are difficult to quantify, the National Center for Computer Crime Data estimates that $550 million is lost annually due to the unauthorized alteration and theft of computer data in this country.[39] While this loss is not trivial, it is nevertheless a mere sixth of the $3 billion spent annually on computer security measures[40] and still smaller than the often quoted

---

39. *See* BUCK BLOOMBECKER, SPECTACULAR COMPUTER CRIMES: WHAT THEY ARE AND HOW THEY COST AMERICAN BUSINESS HALF A BILLION DOLLARS A YEAR (1990) (BloomBecker is the director of the National Center for Computer Crime Data); Evan I. Schwartz & Jeffrey Rothfeder, *Viruses? Who You Gonna Call? "Hackbusters,"* BUS. WK., Aug. 6, 1990, at 71.

40. *See* Schwartz & Rothfeder, *supra* note 39.

estimates placing computer crime losses in the billions of dollars.[41]

On an individual level, the media also exaggerates the quantitative losses related to particular computer crimes. The Hubner and Morris examples discussed in the previous Subsection indicate the magnitude of exaggeration. In the case of Hubner, the media indicated that proprietary information was stolen and national security was breached. In reality, only a few relatively uninteresting items of software were stolen.[42] In the case of Morris, one media account estimated the losses due to Morris's computer worm at hundreds of times their actual value.[43]

2. *Qualitative Misstatement*

In addition to quantitative overstatement, the media also misstates the problem of computer abuse. Computer hackers do not commit the majority of computer crimes. Instead, as much as seventy-five percent of the $550 million annually lost due to computer crime includes "ordinary, white-collar crimes that involve computers."[44] In contrast to the media portrayal, the real threat to computer security involves insiders. But, as previously discussed, fraudulent acts committed by computer users with valid computer privileges do not constitute computer fraud in the strict sense of the term.[45] Standard criminal law proscriptions governing the agency relationship, as well as embezzlement provisions, are sufficient to criminalize such acts. Moreover, computer security is not generally helpful in preventing insider abuse, as inside users are bona fide, legitimate users of particular computer privileges.

It may even be the case that in a world without computer security, the twenty-five percent of the $550 million annually lost to hacker abuses would not significantly increase. The "hacker ethic" of computer use teaches that computers are for creative, not destructive, purposes and that economic motivation misses the point of computing.[46] Thus, "true"

---

41. *See* Hollinger & Lanza-Kaduce, *supra* note 18, at 105-06; John K. Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L.J. 275, 275-76 (1980).

42. *See supra* notes 28-30 and accompanying text.

43. *See supra* notes 31-32 and accompanying text. In the general context of technology abuse, the media has even produced loss estimates at thousands of times their true value. *See, e.g.*, Irwin, *supra* note 10 (describing instance where the *Houston Chronicle* reported government losses of over $12 million in stolen telephone service; the government itself estimated losses of only $10,000).

44. *See* W. John Moore, *Taming Cyberspace*, NAT'L J., Mar. 28, 1992, at 746 (*quoting* BLOOMBECKER, *supra* note 39).

45. *See supra* notes 16-17 and accompanying text.

46. *See* LEVY, *supra* note 7, at 39-49, 65 (describing basic principles of the "hacker

hackers engage in few activities that interest the economic and property-motivated proscriptions of the criminal law. Admittedly, the hacker ethic also maintains that computer networks should be open,[47] and faithful hackers therefore attempt to gain unauthorized access to many different computer systems. But the presence of hackers in systems is not necessarily threatening. Many hackers are not as destructive as much as curious, and this posture makes them less dangerous than the abusive computer insider.

3. *Analysis*

For the purpose of this Article, these media exaggerations are important because they detrimentally affect the development of computer abuse law[48] and the subsequent enforcement of this law.[49] Developing an effective means of addressing the alleged problem of computer abuse requires beginning from the correct factual framework. If legislators, prosecutors, administrators, and others fail to understand the problem of computer abuse, their solutions to the problem may woefully fail. By understanding the computer abuse problem and then objectively asking whether criminal proscription is the most effective means of addressing the issue, one can work towards an appropriate response to the alleged problem. Legislators who effect, modify, and otherwise focus only on the ex post criminalization of computer abuse may be traveling down a dead-end road.

---

ethic"). To be sure, not all hackers adhere to these principles. For example, one computer group in New York, the Masters of Disaster, ardently strived to live up to their name. The five young men that composed this group (Outlaw, Corrupt, Phiber Optik, Acid Phreak, and Scorpion) made a conscious point of violating computer systems. Fortunately, they also made a point of leaving a trail that led to their apprehension in the summer of 1992. *See* Anthony Ramirez, *5 Are Indicted in Computer Credit Theft*, N.Y. TIMES, July 9, 1992, at A14.

47. *See* LEVY, *supra* note 7, at 40.

48. *See* Hollinger & Lanza-Kaduce, *supra* note 18, at 104-07. Florida, the first state to enact a computer crime law, apparently did so in response to a computer crime incident widely publicized by the local media. *See id.* at 106. In fact, "[t]he catalyst for criminalization in over half the jurisdictions that enacted computer crime laws was the media's portrayal of the threat personal computers and modems presented to possessory information." *Id.* at 115.

49. *See* Moore, *supra* note 44, at 746 (indicating prosecutors' fear of crime committed by hackers and questioning raids of computer facilities and seizures of computer equipment during the 150 agent, 24 city raid known as "Operation Sun Devil," conducted by the Secret Service in May, 1990).

II. THE CRIMINAL LAW RESPONSE TO COMPUTER ABUSE

Having investigated the alleged computer abuse problem, this Section looks at the only means presently used to contend with it: state and federal criminal laws. This Section is divided into three Subsections. The first Subsection looks at state computer crime laws. It investigates the failure of traditional state law to address adequately the problem of computer abuse and the legislation created in response to this inadequacy. The second Subsection looks at federal computer crime laws. It examines four areas of federal law that arguably apply to computer abuse: prohibitions against wire fraud,[50] prohibitions against the interstate transportation of stolen property,[51] actions under the Computer Fraud and Abuse Act of 1986 ("CFAA"),[52] and actions under the Electronic Communications Privacy Act of 1986 ("ECPA").[53] The final Subsection explores why there have been few prosecutions under these computer crime laws, even though these laws collectively offer a means to prosecute almost any computer abuse.

A. State Law

With respect to the criminal law, many of the questions that faced state courts during the early stages of computing were not difficult. For example, the issue of whether the unauthorized taking of computer software on disk, tape, or paper constitutes theft is not legally challenging.[54] Because disks, tapes, and paper are tangible and physical forms of property, courts uniformly classified the taking of these items as theft under applicable state statutes.[55] To exclude physical property from the

---

50. 18 U.S.C. § 1343 (Supp. II 1990).

51. 18 U.S.C. § 2314 (1988 & Supp. II 1990).

52. Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. §§ 1001, 1030 (1988 & Supp. II 1990)).

53. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

54. Of course, state courts only have an interest in the theft of computer software in a physical form. The duplication of a computer program itself is subject only to federal copyright law, which preempts concurrent state laws concerning duplication. *See* 17 U.S.C. §§ 202, 301 (1988).

55. *See, e.g.*, National Sur. Corp. v. Applied Sys. Inc., 418 So. 2d 847 (Ala. 1982) (computer programs subject to conversion); Hancock v. Texas, 402 S.W.2d 906, 908 (Tex. Crim. App. 1966) ("It is evident that the computer programs as alleged and the evidence in support thereof show that such property is included and comes within the meaning of the

inclusive sweep of criminal theft for the sole reason that the property involved is technologically advanced would be an arbitrary and unfair result.

In contrast, the determination of whether computing time is property is a hard question. During the 1980s, state courts grappling with this issue generally encountered two factual patterns. First, cases arose involving the unauthorized access of a computer and a subsequent use of computing time thereon. An example of this first model occurs when a computer hacker gains access to a remote (but intrastate) computer system and consumes computing resources.[56] The second group of cases involved the authorized access of a computer for an unauthorized use thereon. An example of this second model occurs when an employee uses an employer's computer for personal use.[57] Although separation of these two models is possible, courts did not make such a distinction. Instead, they viewed both models as presenting the single question of whether computing time is property under applicable state laws of theft.

On first impression, one may think that computer time is property subject to protection from theft. The only value of a computer system is its processing power, and protection against the theft of this processing power is important. The criminal law should broadly define property subject to theft and include computer time within this definition.[58] Three points, however, make this expansive definition problematic. First, the unique nature of computer time creates a factual problem: When excess capacity exists and other (authorized) users are not hurt by the (unauthorized) use of this excess capacity, it is questionable whether something is stolen.[59] Second, there is the legal problem that criminal statutes must be narrowly construed. It is improper to define property in an expansive

---

provisions of the statutes defining the offense of theft.").

56. *See, e.g.*, Lund v. Virginia, 232 S.E.2d 745 (Va. 1977) (student illicitly acquires account on university computer and consumes substantial computer time thereon).

57. *See, e.g.*, Indiana v. McGraw, 459 N.E.2d 61 (Ind. Ct. App. 1984), *vacated*, 480 N.E.2d 552 (1985); New York v. Weg, 450 N.Y.S.2d 957 (N.Y. Crim. Ct. 1982).

58. *See McGraw*, 459 N.E.2d at 65 ("Computer time is services for which money is paid. Such 'services' may reasonably be regarded as valuable assets within the definition of property subject to theft.").

59. *See McGraw*, 480 N.E.2d at 554 (holding that, under Indiana law, an owner of property must be deprived of the benefit of that property and that the unauthorized use in question did not deprive the computer owner of property or interfere with the other users of the computer system). *But see id.* at 555 (Pivarnik, J., dissenting) ("Time and use are at the very core of the value of a computer system. . . . I think it is irrelevant that the computer processed the data from various terminals simultaneously and the limit of its capacity was never reached by any or all of the stations . . . .").

way inconsistent with prior case law excluding time and services from the scope of property subject to theft.[60] Third is the policy rationale that such an expansive definition of property would chill the use of computers. If the unauthorized use of a computer system constituted theft, then employees who used their employers' computers for personal use, even slight, would be subject to criminal prosecution.[61]

Because of these problems, courts declined to include computer time within the definition of property subject to theft. Instead, courts called upon state legislatures to respond to the problem in an appropriate manner.[62] Partly as a result of this judicial invitation and partly because of the fear created by the popular media,[63] state legislatures responded in a dramatic way. As of this writing, only Vermont has not enacted specific laws directed at computer abuse.[64] Although the statutes offer a

---

60. *See Lund*, 232 S.E.2d at 748 ("The phrase 'goods and chattels' cannot be interpreted to include computer time and services in light of the often repeated mandate that criminal statutes must be strictly construed.").

61. *See Weg*, 450 N.Y.S.2d at 961.

> If [the definition] had the broad meaning claimed by the People and included any equipment or facilities serving the function of the owner, the enactment of the revised Penal Law in 1967 would have made criminals of the thousands of employees in government and the private sector who make unauthorized use of their employers' computers, word processors, calculators, copying machines, telephones, typewriters, and other equipment or facilities for personal benefit.

Id.

62. *See id.* ("[T]he Legislature of the State of New York could reasonably find a need to regulate, even by penal sanction, conduct of the type alleged in this [case]. Perhaps computers are a special type of expensive, commonly owned equipment so subject to misuse that the Legislature might wish to give their owners special protection.").

63. *See supra* note 48 and accompanying text.

64. The state statutes include: ALA. CODE §§ 13A-8-100 to 13A-8-103 (Supp. 1992); ALASKA STAT. § 11.46.740 (1989); ARIZ. REV. STAT. ANN. § 13-2316 (1989); ARK. CODE ANN. §§ 5-41-101 to 5-41-107 (Michie Supp. 1991); CAL. PENAL CODE § 502 (West Supp. 1992); COLO. REV. STAT. §§ 18-5.5-101 to 18-5.5-102 (1986 & Supp. 1992); CONN. GEN. STAT. ANN. §§ 53a-250 to 53a-261 (West 1985); DEL. CODE ANN. tit. 11, §§ 931 to 939 (1987 & Supp. 1993); FLA. STAT. ANN. §§ 815.01 to 815.07 (West Supp. 1993); GA. CODE ANN. §§ 16-9-91 to 16-9-94 (1992); HAW. REV. STAT. §§ 708-890 to 708-893 (Supp. 1992); IDAHO CODE §§ 18-2201 to 18-2202 (1987); ILL. ANN. STAT. ch. 38 para. 16D-1 to 16D-7 (Smith-Hurd Supp. 1992); IND. CODE ANN. §§ 35-43-1-4 & 35-43-2-3 (Burns Supp. 1992); IOWA CODE ANN. §§ 716A.1 to 716A.16 (West Supp. 1992); KAN. STAT. ANN. § 21-3755 (1988); KY. REV. STAT. ANN. §§ 434.840 to 434.860 (Michie/Bobbs-Merrill 1985); LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (West 1986 & Supp. 1993); ME. REV. STAT. ANN. tit. 17-A, § 357 (West 1983 & Supp. 1992); MD. ANN. CODE art. 27, § 146 (Supp. 1991); MASS. GEN. L. ch. 266, § 30 (1990); MICH. STAT. ANN. § 28.529 (Callaghan 1990); MINN. STAT. ANN. §§ 609.87 to 609.891 (West 1987 & Supp. 1992); MISS. CODE ANN. §§ 97-45-1 to 97-45-13 (Supp. 1992); MO. REV. STAT. §§ 537.525, 569.093 to 569.099 (1986 & Supp. 1991); MONT. CODE ANN. §§ 45-2-101, 45-6-310 to

variety of perspectives in addressing the issue, all of them criminalize the unauthorized or fraudulent access and use of computer systems; most of them have tiered levels of culpability; many of them provide for additional civil relief; and some even allow for treble damages.

B. Federal Law

While most computer networks of interest to this Article are interstate, state law is limited to intrastate computer crime. Thus, this Subsection looks at two traditional federal statutes, as well as two more recent federal enactments, that address the problem of abuse over interstate computer networks. Like state computer crime statutes, the two new federal laws were enacted in response to the perceived failure of the law to keep pace with technological change.[65]

1. Traditional Law: Proscriptions Against Wire Fraud and Interstate Transportation of Stolen Property

The federal wire fraud law proscribes the use of wire communications

---

45-6-311 (1991); NEB. REV. STAT. §§ 28.1343 to 28.1348 (Supp. 1991); NEV. REV. STAT. ANN. §§ 205.473 to 205.491 (Michie 1992); N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (1986); N.J. STAT. ANN. §§ 2C:20-23 to 2C:20-34 (West Supp. 1992); N.M. STAT. ANN. §§ 30-45-1 to 30-45-7 (Michie Supp. 1989); N.Y. PENAL LAW §§ 156.00 to 156.50 (McKinney 1988); N.C. GEN. STAT. § 14-453 to 14-457 (1986); N.D. CENT. CODE ANN. § 12.1-06.1-08 (Supp. 1991); OHIO REV. CODE ANN. §§ 2913.01, 2913.81 (Anderson 1993); OKLA. STAT. ANN. tit. 21, §§ 1951 to 1958 (West Supp. 1993); OR. REV. STAT. §§ 164.125, 164.377 (1991); 18 PA. CONS. STAT. ANN. § 3933 (Supp. 1992); R.I. GEN. LAWS §§ 11-52-1 to 11-52-8 (Supp. 1992); S.C. CODE ANN. §§ 16-16-10 to 16-16-30 (Law. Co-op. 1985); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 43-43B-8 (1983 & Supp. 1992); TENN. CODE ANN. §§ 39-14-601 to 39-14-603 (1991); TEX. PENAL CODE ANN. §§ 33.01 to 33.05 (West 1989 & Supp. 1992); UTAH CODE ANN. §§ 76-6-701 to 76-6-705 (1990); VA. CODE ANN. §§ 18.2-152.1 to 18.2-152.14 (Michie 1988 & Supp. 1992); WASH. REV. CODE §§ 9A.52.110 to 9A.52.130 (1988); W. VA. CODE §§ 61-3C-1 to 61-3C-21 (Supp. 1992); WIS. STAT. § 943.70 (Supp. 1992); WYO. STAT. §§ 6-3-501 to 6-3-505 (1988).

65. *See* S. REP. NO. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N 3555, 3556 (legislative history of Electronic Communications Privacy Act).

> As Senator Leahy said when he introduced S. 2575 with Senator Mathias, the existing law is "hopelessly out of date." It has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry.

Id. (citation omitted); *see also* Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH., Spring 1992, at 1.

in interstate or foreign commerce to further a scheme or artifice to defraud or falsely obtain money or property.[66] Given the broad scope of the statute, it has been used successfully to prosecute at least two types of computer abuses. First, the statute criminalizes the use of interstate communications to access a computer system and take information therefrom without authorization.[67] Second, the statute criminalizes the use of interstate airline ticket-reservation networks to obtain airline tickets fraudulently.[68] Significantly, this second application does not involve the transfer of the stolen property itself over the communications network. Instead, it criminalizes the mere rearrangement of data in an interstate computer to perpetrate a fraud.

Federal law also proscribes the interstate or foreign transportation of stolen or fraudulently obtained property.[69] Like the federal wire fraud law, this law criminalizes the use of interstate communications to access a computer system and take information therefrom without authorization.[70] This statute, however, differs from the federal wire fraud law in two material respects. On the one hand, the interstate transportation statute is more inclusive than the federal wire fraud law: The interstate transportation statute criminalizes any further transportation of fraudulently obtained information between interstate computers. Two computer criminals communicating via interstate modems are jointly culpable (without use of conspiracy theories), even if only one of the two stole the item of interest.[71] On the other hand, the interstate transportation statute is also narrower than the federal wire fraud law: The interstate transportation statute fails to criminalize the mere rearrangement of data in an interstate computer.

This second limitation makes the interstate transportation statute less generally applicable than the wire fraud statute. Because something must actually be moved over state or foreign boundaries, even if the "something" consists only of electronic impulses over telephone lines, the statute is inadequate to address many crimes committed over interstate

---

66. *See* 18 U.S.C. § 1343 (Supp. II 1990).

67. *See* United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979); United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990); *see also* Friedman, *supra* note 6, at 549-52.

68. *See* United States v. Schreier, 908 F.2d 645 (10th Cir. 1990), *cert. denied*, 111 S. Ct. 787 (1991); United States v. Giovenga, 637 F.2d 941 (3d Cir. 1980), *cert. denied*, 450 U.S. 1032 (1981).

69. *See* 18 U.S.C. § 2314 (1988 & Supp. II 1990).

70. *See Riggs*, 739 F. Supp. 414, 419-23.

71. *See id.*

computer networks. It is preferable to have a statute that seeks to criminalize acts of fraud that happen to occur over computer networks. To this end, the wire fraud statute is an ideal provision to deal with the the problem of computer abuse.

2. *New Law: Computer Fraud and Abuse Act of 1986 & Electronic Communications Privacy Act of 1986*

The Computer Fraud and Abuse Act of 1986 ("CFAA")[72] criminalizes six computer activities: (1) the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or advantage a foreign nation;[73] (2) the unauthorized access of a computer to obtain protected financial information;[74] (3) the unauthorized access of a computer intended for the exclusive use of the federal government;[75] (4) the unauthorized interstate access of a computer system with an intent to defraud;[76] (5) the unauthorized interstate or foreign access of computer systems that results in at least $1000 aggregate damage;[77] and (6) the fraudulent trafficking in computer passwords affecting interstate commerce.[78]

Although the CFAA is inclusive, it nevertheless fails to transcend the already potent wire fraud statute. For example, the fraud provision of the CFAA expressly excludes the unauthorized access of a computer system where "the object of the fraud and the thing obtained consists only of the use of the computer."[79] Thus, as under the wire fraud statute, the mere viewing of data without authorization is not criminal under the CFAA. Furthermore, the protection afforded by the CFAA to national secrets, financial records, and government computers does not require an explicit computer crime statute; protection probably exists irrespective of the provisions of the CFAA.[80] The anti-password provision of the CFAA is

---

72. Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. §§ 1001, 1030 (1988 & Supp. II 1990)). For a detailed description of the CFAA, see Griffith, *supra* note 6, at 474-82.

73. 18 U.S.C. § 1030(a)(1) (1988 & Supp. II 1990).

74. *See id.* § 1030(a)(2).

75. *See id.* § 1030(a)(3).

76. *See id.* § 1030(a)(4).

77. *See id.* § 1030(a)(5)(A).

78. *See id.* § 1030(a)(6)(A).

79. *Id.* § 1030(a)(4).

80. In addition to federal law proscribing wire fraud and the interstate transportation of stolen property, a variety of other federal laws criminalize such conduct, presumably without concern for whether a computer is involved in the crime. *See, e.g.*, 18 U.S.C. §

the most original section of the statute, but to date, there has not been a prosecution under this provision.

In fact, there has been only one successful prosecution under the CFAA in its six year history. In 1991, the Second Circuit upheld the conviction of Robert Morris for his computer worm that resulted in the crashing of numerous university, military, and medical computers around the country on the Internet.[81] The Second Circuit did not address the merits or problems of the CFAA. Instead, it discussed only a technical point concerning the intent requirement under the specific violation charged. The court decided the construction problem, determined that Morris possessed the requisite statutory intent, and affirmed the punishment set by the district court. Significantly, this sentence lacked any period of incarceration. The sentence imposed was relatively light: three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.[82]

The Electronic Communications Privacy Act of 1986 ("ECPA")[83] has never been used to prosecute computer crime, but the seeds of computer crime penalization are nevertheless present. Because the ECPA criminalizes the possession of electronic devices "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications,"[84] computer hackers are concerned that the ECPA could be used to criminalize the ownership of computer modems.[85] While such an interpretation of the ECPA has some merit,[86] it nevertheless lacks

---

798 (1988) (establishing criminal culpability for the disclosure of "classified information," which is broadly defined as including national secrets, to unauthorized persons); 15 U.S.C. § 1681q (1988) (establishing criminal culpability of "[a]ny person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretences. . ."); 15 U.S.C. § 1693n (1988) (establishing criminal culpability for the use of a fictitious, stolen, or fraudulently obtained "card, code, or other device" to effect an interstate electronic fund transfer).

81. *See* United States v. Morris, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991); *see supra* notes 31-38 and accompanying text.

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

83. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

84. 18 U.S.C. § 2512(1)(b) (1988).

85. *See Hacking the Constitution*, L.A. DAILY J., Mar. 27, 1990, at 6.

86. This position is supported by the recent application of the ECPA to cable descramblers, the modified cable "boxes" that intercept satellite signals of cable television providers and give users of the descramblers free cable television service. In the past two years, two circuit courts have held that the ECPA criminalizes the possession of descramblers. *See* United States v. Lande, 968 F.2d 907 (9th Cir. 1992); United States v. Splawn, 963 F.2d 295 (10th Cir. 1992); United States v. McNutt, 908 F.2d 561 (10th Cir. 1990), *cert. denied*, 111 S. Ct. 955 (1991). *But see* United States v. Hux, 940 F.2d 314 (8th Cir. 1991); United States v. Herring, 933 F.2d 932 (11th Cir. 1991) (refusing to apply the

persuasiveness under present views of the "primarily useful" standard. The present rule is that a device is "primarily useful" if the device is expressly designed for illicit conduct.[87] Because computer modems have a number of valid uses, it is unlikely that they would fall under the statute. But the fact that computer users express concern about the possible repercussions of the ECPA does show its deterrent value.

C. Analysis

Ample state and federal law exists to prosecute computer network abuses. Forty-nine of the fifty states and the federal government have recently enacted legislation specifically targeting computer network abuse. Coupled with traditional laws, these new enactments provide a wealth of tools for the prosecution of computer crime. It is hard to imagine that a competent prosecutor could not find at least one criminal sanction under which to prosecute a particular computer abuse.

But, although such a wide variety of law exists, few computer abusers have been prosecuted and those who have been prosecuted have received light sentences.

> If the primary function of the new computer crime statutes was to deter rampant abuse, one would expect the new laws to result in vigorous prosecutions. The number of prosecutions under the new computer crime laws, however, has been surprisingly low, especially when contrasted with the media-created images of rampant abuse by groups of hackers collaborating to share passwords to break into systems. From 1978 to 1986, fewer than 200 criminal prosecutions were initiated nationally. Under the nation's oldest statute, Florida's, fewer than a half-dozen prosecutions had been filed in its first five years. At the same time, some of the most visible offenders . . . who could have become the clearest examples for general deterrence, have been dealt with leniently.[88]

ECPA to cable descramblers). *See generally* Thomas N. FitzGibbon, Note, *Privacy Protection for Programming: Is Modifying Satellite Descramblers a Violation of the Wiretap Law?*, 70 WASH. U. L.Q. 231 (1992).

87. *See* Unites States v. Schweihs, 569 F.2d 965, 969-71 (5th Cir. 1978).

88. Hollinger & Lanza-Kaduce, *supra* note 18, at 117 (citations omitted).

Scant enforcement of the computer crime laws may occur for a number of reasons. Commentators have offered the following hypotheses: The laws may have gaping holes which make enforcement problematic;[89] the laws may be more symbolic than functional;[90] and the present laws may be incorrectly conceived.[91] The first proposal seems incorrect, as laws criminalizing computer abuse have an apparently broad and inclusive sweep. But, although accurate, the second and third proposals are themselves problematic as complete explanations. With regard to the second proposal, the fact that computer crime laws serve a symbolic purpose does not justify the expense of their creation and frequent calls for their amendment. With regard to the third proposal, commentators have suggested that the present criminal laws of A, B, and C are incorrectly conceived, yet the use of hypothetical laws X, Y, and Z would be correct. This suggestion, though, is incomplete.

This third hypothesis, that present computer crime laws are incorrectly conceived, needs to be taken to its logical extreme that any rule of ex post criminalization of computer abuse within the present conception of criminal law will fail to address the problem of computer abuse adequately. As analytically developed in the next Section, the ex post criminalization process does not work very well in the context of cyberspace. To be sure, it is necessary to have computer crime laws to prosecute the occasional computer criminal who does not escape detection, as well as for the government to demonstrate its symbolic posture against the problem. But faith in the ability of computer crime laws to address adequately the problem of computer abuse is misplaced. Similarly, a belief that certain changes to existing computer crime laws will lead to more frequent prosecutions thereunder is not correct. Because the criminal law process does not fit the cyberspace world, a fresh approach is needed.

III. THE FAILURE OF EX POST CRIMINALIZATION OF COMPUTER ABUSE

At least six factors make the ex post criminalization of computer network abuse problematic: (A) the presence of arbitrary spatial

89. *See* Friedman, *supra* note 6.
90. *See* Hollinger & Lanza-Kaduce, *supra* note 18, at 117.
91. *See* Nelson, *supra* note 6.

distinctions in cyberspace; (B) the difficulty of detecting criminal activity in cyberspace; (C) the difficulty of determining criminal identity in cyberspace; (D) the difficulty of proving criminal culpability in cyberspace; (E) the absence of incentives to report computer crime; and (F) the absence of deterrence in present criminal law provisions. Each of these factors is explored in this Section.

A. Arbitrary Spatial Distinctions in Cyberspace

The arbitrary spatial characteristics of cyberspace create problems for criminal law. For example, consider the case of two computer hackers, A and B. Assume that A lives in state X and B lives in state Y. If both hackers gain unauthorized access to a private, non-financial computer system C in state X and both subsequently cause identical damage to this system, A is subject to the laws of state X while B is subject to federal law. The two computer hackers may be subject to very different penalties for identical acts. Although jurisdictional boundaries always create arbitrary legal lines, these lines are particularly arbitrary in the world of cyberspace. The acts in the present example do not occur in separate jurisdictions: They both occur in computer system C.

Traditional criminal law focuses on the situs of the act, which is usually the situs of the actor as well. In cyberspace, though, the situs of the act and actor may not be the same. Because computer crimes instantaneously span a number of jurisdictions, a number of laws could arguably apply. To be sure, the Constitution offers an answer to this choice of law question: The federal government makes law affecting interstate commerce and state governments make law concerning what issues remain.[92] But this division is less than clear in the present case law[93] and it may nevertheless prove problematic in the regulation of cyberspace. For example, how should the law account for computer abuse on a multi-state network where the person who commits the abuse is in-state with the network home but the abusive act produces substantial damage only on out-of-state network nodes? If the boundary between

92. *See* U.S. CONST. art. I, § 8, cl. 3. The states are relatively powerless to regulate issues that the federal government claims fall under the commerce power. *See* Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528 (1985); LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 386-97 (2d ed. 1988).

93. *See* Gregory v. Ashcroft, 111 S. Ct. 2395 (1991) (indicating that federal law preempts traditional state law but only if Congress plainly states such an intent).

state and federal regulation is unclear, such an act could, at worst, completely escape ex post prosecution.

B. Difficulty of Detecting Criminal Activity in Cyberspace

Computer networks are devoid of labels of gender, race, age, national origin, or disability.[94] But with this egalitarian playing field comes the concurrent problem that computer users are almost impossible to identify beyond their chosen (or illicitly obtained) login name. With respect to the criminal law, this quality of computer networks creates three problems: (1) criminal activity is difficult to detect, (2) criminal identity is difficult to ascertain, and (3) criminal culpability is difficult to prove. These three problems are explored in the present and two subsequent Subsections.

Computer networks assume that authorized users are performing authorized tasks. This assumption, however, creates problems for detecting the existence of criminal activity in a computer system. Irrespective of the method of user authentication used in a computer system, unauthorized users gain access to a system by assuming the identity of an authorized user. Thus, the computer system never knows whether a user is authentic or is a person falsely representing himself or herself as an authentic user. Any command issued by a falsely authenticated user is executed as if issued by a truly authorized user. The only method of ensuring that commands are authentic is ensuring that users are authentic.

And while the use of more rigorous user authentication would reduce the problem,[95] the criminalization of computer abuse is unrelated to standards of user authentication. Irrespective of the quality and completeness of law criminalizing computer abuse, it is impossible to punish acts that escape detection. Because the now-prevalent method of user authentication is the password, the dearth of computer crime prosecutions is not surprising. The problem rests in the authentication of the user, not in the laws available to punish unauthorized users.

Notwithstanding this user authentication problem, the detection of crime in cyberspace is complicated for a second reason: Cyberspace is

---

94. *See* LEVY, *supra* note 7, at 43 (emphasis omitted) (noting that the hacker ethic includes the belief that "[h]ackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position"); Cutrera, *supra* note 1, at 139.

95. *See supra* notes 13-14 and accompanying text (describing techniques of encryption, call-back, and biometric or mechanical user authentication).

devoid of physical property limitations. Because computer data is freely replicable, information can be stolen without altering or removing such information from its source. As the mere replication of information is difficult to detect on most computer systems, the theft of valuable intangible property may entirely escape detection.

C. Difficulty of Determining Criminal Identity in Cyberspace

Even when a computer crime is discovered, the inability to ascertain the identity of the computer criminal also leads to the present lack of ex post prosecutions of computer abuse. Because computer criminals are identifiable only through their illicit login names, they enjoy an anonymity rarely present in criminal activity. For remote computer abuse, the only source tracing a computer criminal to a particular computer abuse is the phone from which the criminal gains unauthorized access to the system. If the criminal can hide this information,[96] he or she may completely escape identification.

The identification problem is compounded by a second characteristic of computer systems: Computer criminals can acquire chameleon-like identities by routinely changing passwords. An insider computer criminal can steal the passwords of a number of fellow employees and obtain many false identities. Similarly, a remote computer criminal can obtain a small library of passwords relatively easily and thereby become difficult to identify.[97] Especially under password systems of user authentication, the link between user and authentication is so inconsequential that it is easy for one to assume an array of identities in cyberspace. The identification of the criminal adds an entire layer of complexity to the problem of

---

96. *See supra* note 23 and accompanying text.

97. *See supra* note 26 and accompanying text. An employee of Digital Equipment Corporation described Kevin Mitnick's computer invasions in terms that vividly capture the detection problem.

> We seem to be totally defenseless against these people. We have repeatedly rebuilt system after system and finally management has told the system support group to ignore the problem. As a good network citizen, I want to make sure someone at network security knows that we are being raped in broad daylight. These people freely walk into our systems and are taking restricted, confidential and proprietary information.

CYBERPUNK, *supra* note 22, at 120. Significantly, the quoted employee refers to Mitnick in the plural, unable to surmise that the repeated invasions of Digital's systems were not the work of a group of computer hackers.

discovering the abuse.

D. Difficulty of Proving Criminal Culpability in Cyberspace

But even where computer abuse is detected and an unauthorized actor is associated with the abusive act, it is still difficult to prove criminal culpability in cyberspace. In the electronic world of cyberspace, many of the traditional criminal law elements of proof are nonexistent. For example, an eyewitness cannot give an account of a computer criminal running into the system with a weapon, nor can a positive identification be given from a police line-up. Without going into every factual complication, let it suffice to say that computer criminals do not leave fingerprints. The unusual spatial character of cyberspace makes obsolete many methods of associating the criminal with the crime.

Collection of evidence from computer systems also raises important privacy concerns.[98] Presently, the scope of Fourth Amendment protection for computer files, electronic mail, and other digitized information is not clear,[99] but such electronic information is nevertheless protected under the ECPA.[100] These privacy expectations frustrate the criminal process by making the collection of evidence difficult. As one commentator stated, "[h]ow you obtain the evidence you need and yet protect the privacy concerns and the confidentiality of any other information on the computer system is very tricky."[101] Law enforcement officials must selectively investigate the files and data of fraudulent users while respecting the privacy rights of authorized users. This task is particularly difficult when a computer hacker assumes the identity of an authorized user working with highly confidential information because officials must parse the criminal from the legitimate within a single user's files.

---

98. *See* S. REP. NO. 541, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S.C.C.A.N 3555, 3559; Moore, *supra* note 44, at 747-48.

99. Because the law does not focus on the medium of storage as much as it focuses on users' expectations of privacy, *see* Katz v. United States, 389 U.S. 347, 351 (1967), it is likely that some protection exists for computerized data. The use of user authentication to restrict computer access demonstrates that computer users believe that systems are private and shows that they do not expect others to access their files without authorization. *But see* Ruel T. Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 24-27 (1988) (arguing that little or no privacy protection existed prior to the ECPA). Professor Tribe argues that the Constitution should be amended to clearly establish the right of privacy (and other constitutional rights) in cyberspace. *See* Tribe, *supra* note 1, at 23.

100. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

101. Moore, *supra* note 44, at 748 (statement of Donn B. Parker).

E. Absence of Incentives To Report Computer Abuse

In addition to the problem of prosecuting computer abuse once it is discovered, economic incentives encourage the victim to prevent its discovery. This effect occurs for two reasons. First, criminal prosecution of computer abuse fails to compensate the victim for damage done to his or her computer. Second, victims of computer abuse do not want to disclose the fact that their networks were compromised; such disclosures may have adverse economic effects on the victims. Disclosure of a network security breach is embarrassing particularly where the computer crime victim maintains (theoretically) confidential financial records or is itself involved in the computer industry.[102]

Because of these economic disincentives to reporting computer abuse, some suggest that the CFAA[103] should be amended to include a civil cause of action for the purpose of increasing the frequency of reporting.[104] In fact, Congress has considered legislation having this precise effect, but as of this writing, such legislation has not been enacted.[105] The problem with this proposal, however, is that there are no incentives to initiating civil actions. Computer criminals are generally individual actors with finite resources. It does not make sense for a corporation to initiate a suit against a private actor with shallow pockets, for litigation costs exceed potential returns. Moreover, insurance is not a viable alternative because individual actors do not carry liability insurance for the commission of computer crimes.

F. Absence of Deterrence in Present Criminal Law Provisions

As a final point, the present law fails to provide sufficient deterrence to eliminate the problem of computer abuse. Although this point is circular, it is nevertheless significant that only a few computer prosecutions have been successful.[106] A potential computer criminal sees

---

102. *Cf. id.* at 746 ("[C]ompanies worry more about the loss of public trust than about the loss of money" from computer abuse).

103. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. §§ 1001, 1030 (1988 & Supp. II 1990)).

104. *See* Griffith, *supra* note 6, at 489.

105. *See* Computer Abuse Amendments Act of 1991, S. 1322, 102d Cong., 1st Sess. (1991) (pending); *see also* Crime Control Act of 1992, S. 2305, 102d Cong., 2d Sess. (1992) (not enacted); Violent Crime Prevention Act of 1991, H.R. 3371, 102d Cong., 1st Sess. (1991) (not enacted).

106. *See supra* note 88 and accompanying text.

computer laws that have much "bark" in theory but that have little "bite" in practice. Until a computer criminal is incarcerated under the CFAA, this law lacks meaningful deterrent value. For this and the other reasons discussed in this Section, it is appropriate to focus attention away from the ex post criminalization of computer abuse and to turn to an alternative mode of analysis.

IV. EX ANTE PREVENTION OF COMPUTER ABUSE AS AN ALTERNATIVE

If the ex post criminalization of computer abuse is not a viable method of addressing the alleged problem of computer abuse, then a practical alternative is the implementation of ex ante measures to keep the problem from occurring. The best means for realizing a preventive scheme is through the use of advanced computer security.[107] In particular, the most problematic aspect of present computer system security is the use of password user authentication. To the extent that more sophisticated means of user authentication are used, the probability of unauthorized use decreases and the frequency of computer abuse declines. If a system could theoretically screen out all unauthorized users, the problem of computer abuse would be nonexistent.[108]

This Section is divided into three Subsections. The first two Subsections propose methods of encouraging the increased use of sophisticated computer security. The first Subsection suggests a method involving direct federal regulation, and the second Subsection suggests a method involving indirect federal regulation. The final Subsection, however, questions whether technology forcing measures, such as those proposed in the first two Subsections, are appropriate responses. In particular, this Subsection examines the hypothesis that the market for computer security equipment should establish an efficient level of spending on computer

---

107. Although Griffith, *supra* note 6, at 487, encourages the adoption of legislation to increase computer security, he recommends this change as an amendment to the CFAA instead of as an alternative paradigm. Other commentators have also suggested the need to increase computer security to decrease computer crime. *See, e.g.*, Stanley L. Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER/L.J. 353, 368-71 (1980). But neither of these commentators suggests that the criminal law is a less than adequate vehicle for eradicating computer abuse nor do they offer the analysis proposed in this Section for viewing the alternative paradigm of ex ante prevention.

108. Recall that abusive acts by authorized users are not computer abuses in the strict sense of the term. *See supra* notes 16-17 and accompanying text.

security equipment with a resulting efficient level of loss through computer abuse. In contrast to the popular perception that computer abuse is rampant, it may even be the case that losses from computer abuse are inefficiently low and that increased spending for computer security equipment should be discouraged rather than encouraged.

A. Direct Regulation: Establishing Security Requirements on the National Research and Education Network

As part of the High-Performance Computing Act of 1991,[109] Congress established a plan to construct the National Research and Education Network ("NREN"),[110] a national high-speed fiber optic communications network. The NREN is intended to replace the NSFNET, the principal component of the Internet.[111] By its projected completion in 1996, the NREN will link as many as 1300 institutions and a million researchers nationwide and will be able to carry data at speeds approximately 2000 times faster than the present NSFNET.[112] Congress believes that the construction of such a national, high-speed data communications network is instrumental to the utilization of super computing technology in the United States.[113]

The NREN program offers an excellent opportunity for the establishment of uniform security requirements on a national network. In fact, legislation even requires the establishment of security requirements as part of the overall program.

> The President shall implement a National High-Performance Computing Program, which shall . . . provide . . .
>
> (i) for the security requirements, policies and standards necessary to protect Federal research computer networks and information resources accessible through Federal research computer networks, includ-

---

109. Pub. L. No. 102-194, 105 Stat. 1594 (codified at 15 U.S.C.A. §§ 5501-28 (West Supp. 1992)).

110. *See* 15 U.S.C.A. § 5512 (West Supp. 1992).

111. *See* S. REP. NO. 57, 102d Cong., 1st Sess. 9-10 (1991), *reprinted in* 1991 U.S.C.C.A.N. 1228, 1236-37.

112. *See id.*

113. *See* 15 U.S.C.A. §§ 5501-02 (West Supp. 1992); S. REP. NO. 57, 102d Cong., 1st Sess. 3 (1991), *reprinted in* 1991 U.S.C.C.A.N. 1228, 1230.

> ing research required to establish security standards for high-performance computing systems and networks; and
>
> (ii) that agencies and departments identified in the annual report submitted under paragraph (3)(A) shall define and implement a security plan consistent with the Program and with applicable law.[114]

By requiring the use of sophisticated security systems for nodes on this network, the NREN program could ensure that very few instances of computer abuse occur on this forthcoming data highway. The NREN program, however, should also be cognizant of the costs such sophisticated security requirements impose, and it should weigh these costs against the benefits of reduced computer abuse. As a result of this weighing process, the NREN program may conclude, for example, that continued adherence to the password system of user authentication is outdated and that serious consideration should be given to requiring sophisticated systems of user authentication on computers containing confidential, secret, or proprietary data. The NREN program may also find it helpful to solicit the advice of leaders in the computer industry to determine cost-efficient levels of spending for computer security. The important contribution of this Article is that the debate over security measures should be conducted with an understanding that computer crime laws will not significantly deter future computer abuse.

B. Indirect Regulation: Tax Incentives for Increasing Computer Security

Even if the NREN program adopts regulations leading to efficient levels of computer security spending, there will nevertheless be local area networks ("LANs") that will not be linked to the NREN nor subject to its regulation. Thus, a different solution is required to address the

---

114. 15 U.S.C.A. § 5511(a)(2)(I) (West Supp. 1992). The reporting agencies and departments include the Department of Agriculture, the Department of Commerce, the Department of Defense, the Department of Education, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Environmental Protection Agency, the National Aeronautics and Space Administration, the National Science Foundation, and any others considered appropriate. *Id.* § 5511(a)(4)(B).

problem of computer security on LANs. Moreover, any federal solution to this problem must also address the problem of federalism. Because federal law cannot directly encroach upon the regulatory power of states over intrastate computer networks,[115] indirect federal legislation must provide the answer.[116] The federal spending power is one popular method through which federal power can be indirectly exercised to influence state legislation.[117] But in the context of computer abuse, the federal taxation power[118] offers a preferable solution: the taxation power is self-contained and avoids the problem of requiring further state legislation tied to federal funds appropriations.

The federal taxation power can be used to increase computer security in two ways. First, producers of computer security equipment could be given favorable tax treatment, which would result in an increase in the supply of affordable computer security equipment. Alternatively, consumers of computer security equipment could be given incentives to invest in such equipment, which would result in an increase in the demand for security equipment. In either case, favorable tax treatment results in a government subsidy to the industry, and before such a subsidy should be given, it must be justified. Thus, it must be shown that current spending levels on computer security equipment are inefficiently low and that a subsidy is needed to produce the efficient level of spending.

C. Analysis

The first two Subsections propose methods for encouraging investment in computer security equipment. But encouraging such investment is premised on the assumption that the market for computer security equipment is not producing sufficient investment. In this market, the primary cost is the cost of investment in security-related equipment, and the primary benefit is the reduction in loss from computer abuse that the security equipment produces. Thus, investment in computer security

---

115. *Cf. supra* notes 92-93 and accompanying text.

116. *See* South Dakota v. Dole, 483 U.S. 203 (1987) (upholding program of tying five percent of a state's highway funds to its enactment of minimum drinking age requirement of 21 years); *see* TRIBE, *supra* note 92, at 321-23.

117. *See South Dakota*, 483 U.S. at 206 ("Here, Congress has acted indirectly under its spending power to encourage uniformity in the States' drinking ages. . . . [W]e find this legislative effort within constitutional bounds even if Congress may not regulate drinking ages directly.").

118. *See* TRIBE, *supra* note 92, at 318-20.

equipment should be encouraged if market participants either overestimate the costs of the equipment or underestimate the benefits of investment in security equipment. These conditions, though, are not present in the market. Although the analysis given here is not intended to be exhaustive of the issue, there is no reason to believe that the market for computer security equipment encourages underinvestment.

For each dollar lost on computer abuse, approximately five dollars are spent for computer security equipment.[119] Moreover, if one looks only at computer abuses that are not white-collar crimes involving computers, then the ratio increases from one dollar lost on computer abuse to approximately twenty dollars spent for computer security equipment.[120] For increased spending on computer security equipment to be justified, the marginal benefits of decreased computer abuse must be greater than the marginal costs of increased computer security spending. In other words, for each additional dollar spent on computer security equipment, this cost would have to be justified by more than a dollar decrease in computer abuse. Although it is beyond the scope of this Article to examine the marginal costs and benefits of increased spending on computer security equipment empirically, it seems unlikely that additional spending on computer security equipment is justified.

If anything, spending for computer security equipment is probably already too great. This situation exists if the marginal costs of increased computer abuse are less than the marginal benefits of decreased computer security spending from present levels of spending for security equipment. Given the disproportionate ratio of investment in security equipment to levels of computer abuse, one suspects that overinvestment in security equipment does occur. Moreover, this impression of the problem is reinforced by at least two effects. First, the media exaggerates the scope and magnitude of losses from computer abuse.[121] If the market relies on this incorrect information, then overinvestment in security equipment is likely to occur. Second, many consumers show irrational fears of computer failure and susceptibility to abuse. Thus, even if the level of spending for computer security equipment by large, informed, institution-

---

119. *See supra* notes 39-40 and accompanying text ($550 million annually lost to computer abuses and $3 billion spent annually on computer security equipment).

120. *See supra* notes 39, 40 & 44 and accompanying text (noting that as much as 75% of alleged computer abuses are mere white-collar crimes that happen to involve computers). Thus, the ratio of ($550 million x 25%) to $3 billion reduces to about $1 to $20.

121. *See supra* notes 39-47 and accompanying text.

al computer users is at an efficient level, smaller computer users may nevertheless be overinvesting in computer security equipment.

The present analysis must be refined and expanded. But before such study is feasible, more complete empirical data about losses from computer abuse and investment in computer security equipment is needed. Moreover, secondary costs and benefits should also be introduced into the calculus. For example, two important secondary factors are the amount of time lost to installing, maintaining, and using computer security equipment and the amount of investment in computer abuse monitoring. The goal of this Article is not to make a complete economic evaluation of the computer security market on the basis of incomplete information. Instead, the goal of this Article is to shift the policy debate about computer abuse towards these types of market questions, with an understanding that criminal proscriptions against the commission of computer abuse are an insignificant factor in the analysis.

CONCLUSION

The computer abuse problem is more a media contrivance than a source of real economic loss in this country. At present, legislatures have shared the media's anxiety and have responded to the alleged problem of computer abuse with a wealth of laws criminalizing abusive acts committed on networked computers. For a number of reasons, though, this response is not helpful in addressing the problem, even assuming that a problem exists. Because the ex post criminalization of computer abuse faces problems of jurisdiction, detection, proof, and deterrence, it is useful to investigate alternative means of addressing the alleged problem.

On making this inquiry into alternatives, one discovers that a practical and effective way of addressing the issue of computer abuse is through its ex ante prevention. In particular, the use of sophisticated methods of user authentication decreases the likelihood of unauthorized access and therefore decreases the frequency of computer abuse. The benefits of decreased computer abuse, however, must be weighed against the costs of increased computer security measures. If the costs of increasing computer security are indeed justified, the federal government could impose mandatory security requirements on all interstate networks, such as the NREN, or it could tamper with the market for computer security equipment through its taxation power. These somewhat drastic steps, however, are not appropriate until it is first established that there is

market failure in the market for computer security equipment.

In summary, this Article urges that the question to ask with regard to addressing the alleged problem of computer abuse should not be "How can we amend ineffectual computer crime laws?," but rather, "Given the limitations of any scheme of ex post criminalization, is the market for computer security equipment a well functioning market?" Only through an investigation of this latter question will meaningful progress be made.