University of Arkansas at Little Rock Law Review

Volume 10 | Issue 1 Article 4

1987

What is Computer Crime, and Why Should We Care

Michael C. Gemignami

WHAT IS COMPUTER CRIME, AND WHY SHOULD WE CARE?*

*Michael C. Gemignani***

The heightened concern over computer crime is evidenced by the increasing number of professional organizations which have conducted studies to determine how much computer crime there really is and who is committing it.[1] Even with these studies, no one is yet able to say with any certainty how much computer crime there is and how much of a threat it poses. Nevertheless, the federal government and most states now have statutes which specifically address computer abuses.[2] There is also a broad array of other criminal statutes which can be used as weapons against the computer criminal.[3]

There are two major reasons for the confusion surrounding computer crime. One is that there is still no universally accepted defini-

---

* This article is based on a lecture given as part of the first Altheimer Foundation Law, Science and Technology lecture series. The lecture was given at the University of Arkansas at Little Rock on March 12, 1986.

** Dr. Michael C. Gemignani is currently serving as Dean of the College of Arts and Sciences, University of Maine. He is a member of the Indiana and Maine Bars and received his J.D., summa cum laude, from Indiana University School of Law. Dr. Gemignani has a Ph.D. in mathematics from the University of Notre Dame and did his undergraduate work at the University of Rochester. He was formerly Dean of the College of Sciences at Ball State University.

1. ERNST & WHINNEY, COMPUTER FRAUD (1987) (report presented to the National Commission on Fraudulent Financial Reporting); *First Annual Statistical Report of the National Center for Computer Crime Data*, COMPUTER CRIME, COMPUTER SECURITY, COMPUTER ETHICS (J. Bloombecker ed. 1986); TASK FORCE ON COMPUTER CRIME, A.B.A. SECTION OF CRIMINAL JUSTICE, REPORT ON COMPUTER CRIME (1984) [hereinafter ABA REPORT]; R. Kusserow, Computer Related Fraud and Abuse in Government Agencies (1983) (report ordered by the President's Council on Integrity and Efficiency). Donn Parker of Stanford Research Institute conducted one of the earliest surveys of computer crime. It was released in 1973 as a report, *Computer Abuse*, co-authored by Parker, Susan Nycum and Stephen Dura. Also, the results are summarized in D. PARKER, CRIME BY COMPUTER (1976), which describes several early instances of computer crime.

2. Thackery, *Computer-Related Crimes, An Outline*, 25 JURIMETRICS J. 300, 316-17 (1985). In 1985, 36 states had computer crime statutes. Congress passed the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" as a rider to a budget bill at the end of the 98th Congress. Pub. L. No. 98-413, § 2102(a), 98 Stat. 2190 (1984). The Act amends chapter 47 of title 18 of the United States Code by adding a new section, § 1030, which specifies three rather narrowly drawn categories of computer crime. 18 U.S.C.A. § 1030 (West Supp. 1986). Other federal computer crime legislation is currently pending before Congress.

3. *See, e.g.*, Nycum, *The Criminal Law Aspects of Computer Abuse, Part II: Federal Criminal Code*, 5 RUTGERS J. OF COMPUTERS & THE LAW 297 (1976).

tion of computer crime, although some have been suggested.[4] The second is that there is no agreement concerning how much computer crime is acutally detected, or, even if detected, what damages result from such crime.[5]

The ambivalent attitude toward computer crime is exemplified by the reluctance sometimes shown by police and prosecutors to pursue the computer criminal.[6] The technology requires special expertise, and preparation of a case against a suspect can be time-consuming and tedious.[7] The computer criminals often seem more clever than dangerous, and the victims are more likely to be large businesses or banks rather than flesh-and-blood human beings. Perhaps nowhere, however, is the ambivalence toward computer crime demonstrated more forcefully than in the courts. All too often indictments for computer crime have been dismissed because the "criminal" act was held not to be covered by the statute under which

4. A classic work which categorizes types of computer abuse is D. PARKER, *supra* note 1, at 12-22. *See also*, Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681 (1980). This author believes that the term computer crime should be reserved for traditional crimes which have acquired a new dimension or order of magnitude through the aid of a computer, and abuses which have come into being because of computers.

5. *See* Gemignani, *supra* note 4, at 686-87. If a state computer operator deletes a friend's DWI conviction from the files of the Bureau of Motor Vehicles, then what is the value of the loss suffered? If an office worker illicitly copies a copyrighted program used at work for use at home but would not have been able to afford his own copy of the program and, therefore, would never have purchased a copy, what is the value of the damage brought about by this "crime"?

6. ABA REPORT, *supra* note 1, at 148 notes that of 148 respondents who experienced incidents of computer crime, 50 of these did not report any of the incidents to law enforcement agencies. Only 40 of the 148 reported all such incidents to the authorities. *Id.* at 21. There were 143 respondents who took action against an identified perpetrator. The results are ambiguous since multiple responses were allowed. No action was taken in 39 of the instances. In 49 cases, a criminal investigation was underway or completed. Prosecution began in 54 cases, but only 15 of those cases resulted in a fine or prison term or both; 21 were still pending. What is perhaps more remarkable is that in less than half of the cases did the employer take any disciplinary action against the perpetrator. If prosecutors are unwilling to pursue computer crime vigorously, employers may be even less aggressive.

7. *See, e.g.*, the account of the case of John Thommen discussed in Gemignani, *supra* note 4, at 713 (citing State v. Thommen, No. 79-424B (Crim. Ct. Marion Co., Ind. Feb. 14, 1980)). The state police officer who investigated the case spent literally hundreds of hours collecting evidence from computer-generated logs. *Id.* Thommen received two years probation and a $500 fine. Jerry Schneider, who allegedly stole more than a million dollars worth of equipment from the phone company using a computer, served forty days and paid a $500 fine. *See* D. PARKER, CRIME BY COMPUTER (1976). Stanley Mark Rifkin was able to transfer more than $10 million via computer from the Pacific National Bank to an account in New York that he controlled. He used the money to buy more than $8 million worth of diamonds from the Russians. He received a seven-year term but only because he tried the same trick again while awaiting trial. For an account of the Rifkin case, see Becker, *Rifkin, A Documentary History*, 2 COMPUTER/LAW J. 471 (1980).

charges were brought. When this first hurdle is overcome, the sentences imposed in successful prosecutions seem hardly to justify the effort taken to prepare the case.[8] It is the former issue that I will discuss in this article: How have courts tried to shape the nature of computer crime by refusing to allow prosecution under statutes which, at first reading, seem applicable? I consider first a 1985 case from Indiana, *State v. McGraw*.[9]

Michael McGraw was a computer operator for the Indianapolis Department of Planning and Zoning, which rented a computer from Marion County on a flat fee basis. For his private business involving the sale of the diet product known as NaturSlim, McGraw used the city's computer for client lists, inventory control, copies of solicitation letters, and other materials related to the enterprise. McGraw had no authorization to use the computer in this way. In fact, he was repremanded for carrying on his private business on office time and was later fired for refusing to stop this activity as well as for allegedly substandard performance.

Shortly after he was fired, McGraw asked a fellow employee, another computer operator, to obtain a printout of his NaturSlim data and then to erase it from the computer's memory. Instead of complying, the operator informed his supervisor, and the resulting investigation showed the scope of McGraw's activities. The printout of the NaturSlim data amounted to a sheaf of computer paper four to five inches thick.

McGraw was charged with theft under the Indiana Criminal Code section 35-43-4-2(a) which states: "A person who knowingly or intentionally exerts unauthorized control over property of another person, with intent to deprive the other person of any part of its value or use, commits theft, a class D felony."[10] According to the Indiana Code, "Property means anything of value;" and includes "[a] gain or advantage or anything that might reasonably be regarded as such by the beneficiary;" it also includes services.[11]

McGraw was convicted of theft, but the trial court granted his post-trial motion to dismiss on the grounds that the counts against him did not state an offense against the State of Indiana over which the court had jurisdiction. The State appealed.

The Indiana Court of Appeals narrowed the issues to one ques-

8. *See* sources cited *supra* note 4.

9. 459 N.E.2d 61 (Ind. App. 1984), *vacated*, 480 N.E.2d 552 (Ind. 1985).

10. IND. CODE ANN. § 35-43-4-2(a) (Burns 1985).

11. *Id.* § 35-41-1-23 (Burns 1985).

tion: Whether the unauthorized use of another person's computer for private business is theft under the statute as a matter of law.

McGraw argued that the word "use" does not appear in the theft statute, which, instead, relies upon "unauthorized control." He also noted that the definition of property does not refer to use and that the services specifically mentioned as property concern labor rather than electronic data processing. He maintained that he could not deprive the city of the "use" of its computer unless "his data caused an overload on the computer memory banks, or that he used the computer for his private business at a time which interfered with city's use."[12] Finally, he argued that the value of the services were de minimis, no more than the value of the personal use of an office phone, calculator or copy machine. The court of appeals, however, stated that, since it was clear that McGraw knowingly and intentionally used the computer for his own monetary gain, the only question was whether the use of a computer was property subject to theft.[13]

The court reviewed several cases, two of which we will review later in this article,[14] but found them inapplicable. It concluded that McGraw's interpretation of the applicable statutes was too restrictive. He was asking the court to accept an outdated common law notion of larceny; modern statutes had gone beyond this notion as mandated by modern technology. The taking of electricity and cable television service had already been found to be grounds for a charge of theft in Indiana.[15]

The court of appeals found that, since computer time is something for which money is paid, it can reasonably be regarded as a valuable asset. If a person takes such services, he exerts control over them. Depriving the other person of any part of the services' use without authorization completes the elements needed for theft. The court rejected McGraw's argument that, because his use of the computer did not interfere with its normal operation, his conduct was not criminal.[16] The Indiana Supreme Court then agreed to hear the case.[17]

The Indiana Supreme Court noted that criminal statutes must be construed strictly against the state. The theft statute did not distin-

12. 459 N.E.2d at 64.

13. *Id.*

14. *See infra* notes 27-30, 33-35 and accompanying text.

15. Helvey v. Wabash County REMC, 151 Ind. App. 176, 278 N.E.2d 608 (1972) (electricity); Moser v. State, 433 N.E.2d 68 (Ind. App. 1982) (cable television service).

16. 459 N.E.2d at 65.

17. State v. McGraw, 480 N.E.2d 552 (Ind. 1985).

guish between use of another's property for monetary gain and its use otherwise, so the court could not apply that distinction.

McGraw was provided a computer terminal at his desk and computer storage for his own use. The court found that, although McGraw's supervisor either knew or suspected that McGraw was using the computer for private business, the supervisor never investigated or reprimanded McGraw for such use, and McGraw's use was not cited as a basis for his discharge. McGraw even received unemployment benefits after his firing.

The court was willing to assume that McGraw's use of the computer was unauthorized and that use of a computer is property. However, the harm that the theft statute attempts to prevent is depriving a person of the use of his property; the harm is not centered in "a benefit to one which, although a windfall to him, harmed nobody."[18] The central question then is not, as the court of appeals suggested, "Is computer time subject to theft," but rather, "who was deprived of what?"[19]

The computer was leased to the city at a fixed fee. The tapes and disks on which data were stored were erasable and reusable. The capacity of the time-sharing system was never approached so no legitimate user was ever denied access to the use of the computer. "Defendant's unauthorized use cost the City nothing and did not interfere with its use by others. He extracted from the system only such information as he had previously put into it."[20] The court found no distinction between McGraw's actions and an employee's use of a stenographer's typewriter to write personal letters or the use of vacant space on a company bookshelf to store personal belongings.

The court concluded: "[W]hen the natural and usual consequences of the conduct charged and proved are not such as would effect the wrong which the statute seeks to prevent, the intent to effect that wrong is not so inferrable."[21] Because the city was not deprived of anything, the intent to effect a deprivation must be proved. No such proof was offered.[22] The court suggested that if McGraw was guilty of anything, it would have been only criminal conversion, which does not require intent "to deprive the other of any part of the article's value or use."[23]

18. *Id.* at 554.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.* at 554-55.
23. *Id.* at 555 (citing IND. CODE ANN. § 35-43-4-3 (Burns 1985)).

The Indiana Supreme Court seemed to be saying that if someone can find a way to use the property of another without inconveniencing that person, then he or she has not committed theft. True, the court left open the possibility of prosecution for criminal conversion, but this sharply diminishes the seriousness of the offense. If I take your car from the parking lot at your place of business, use it all day, and then return it before you need it to return home, have I not stolen your car? Certainly not under the common law notion of larceny where I had to have the intent to deprive you of your car permanently, but I would certainly have "stolen" your car under the current Indiana Criminal Code. Or would I have? Perhaps not, according to the Indiana Supreme Court's ruling in *McGraw*.

It seems, according to the Indiana Supreme Court's logic, that whether or not one steals through unauthorized use of a computer system depends upon accidental circumstances rather than the act itself. Suppose that it could be proven that McGraw's unauthorized activities inconvenienced legitimate users of the city's computer system in a minimal way such as by slowing response time by a small but perceptible amount.[24] Would this have been sufficient to find a deprivation of use? Or suppose that McGraw had erased legitimate files, even accidentally, when he created his own illegitimate ones. Would there then have been a deprivation? Indeed, even if McGraw had used data from city-owned files for his private business, who would have been deprived of anything? The files themselves would remain in computer storage; only the information in them would have been used. Do we then condone unauthorized taking of confidential data because the owner of the data still has it after the taking has been accomplished?

Can a computer system properly be compared with other tools such as a hammer or a telephone? True, one can do mischief with a hammer or make obscene calls with a telephone, but these devices do not have the same power or potential for abuse as does a computer. We do not store secret data or vast assets in our telephones, and the damage we can do with a hammer is relatively localized and dependent in large measure upon our strength and reach. Misuse of a computer can cause immense damage,[25] and even when damage does not,

24. The "response time" is the time that elapses between an operator's sending a command to a computer and the time the response to the command appears at the operator's terminal. C. SIPPL, MICROCOMPUTER DICTIONARY AND GUIDE 390 (1976). If McGraw's activity had increased response time by 0.01 of a second, then it would have taken 6000 terminal transactions to cost the city one minute of work time.

25. The estimates of the overall computer losses caused by computer crime vary so widely

in fact, materialize, the potential consequences of intentional misuses are still significant.[26] For a court to place a computer on a par with a typewriter or a bookcase, as did the Indiana Supreme Court, shows a serious misunderstanding of the power of computers and their role in today's society.

The Commonwealth of Virginia displayed an antiquated notion of theft in a case involving Charles Lund, a graduate student in statistics, who was using the computer at Virginia Polytechnic Institute and State University (VPI).[27] Lund needed to use VPI's computer, a machine leased from IBM, in his research, but his advisor failed to obtain an account for him. Lund used the computer anyway, charging his work to other accounts whose access codes he had obtained. Although legitimate accounts were billed for the use of the computer, no money actually changed hands. The billing was merely a bookkeeping device to apportion the rent paid to IBM according to how much a department used the machine. Lund's activity was brought to light when various users complained that unauthorized charges were made on their accounts. Lund was confronted, and he eventually admitted his activity. He was charged with grand larceny under statutes which required that he "obtained, by any false pretense or token, from any person, with intent to defraud, money or other property which may be the subject of larceny" having a value of one hundred dollars or more.[28] The director of VPI's computer center estimated the value of what Lund had taken at more than $25,000.

Despite testimony from several faculty members, including his department chair and thesis advisor, that the work Lund had done on the computer was legitimate academic research and that he would have been given a computer account had he asked for one, Lund was

---

as to call any estimate into serious question. An ABA Report notes published estimates between $20 million and $5 billion annually. ABA REPORT, *supra* note 1, at 38.

26. Susan Nycum, one of the nation's most respected computer lawyers, told a Congressional committee of an event that occurred when she was director of a computer center. Someone attempted to erase a key file directory using a telephone link to the computer. Although an alert operator disconnected the caller before any damage was done, had the would-be vandal been successful, it would have cost approximately $50,000 to undo the damage. *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Crim. Laws & Proc. of the Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 70 (1978). A more recent threat has been the placement of seemingly useful programs on electronic bulletin boards; the programs actually contain treacherous "logic bombs," *see infra* note 38, that can destroy a user's data and cause other problems. This has made many people wary of using software that is found on electronic bulletin boards or that comes from an unknown source. This, in turn, inhibits the free flow of information among computer enthusiasts.

27. Lund v. Commonwealth, 217 Va. 688, 232 S.E.2d 745 (1977).

28. VA. CODE ANN. § 18.2-178 (1982).

convicted of grand larceny. He appealed to the Supreme Court of Virginia.

At the time, Virginia used a common law definition of larceny, defining it as "the taking and carrying away of the goods and chattels of another with intent to deprive the owner of the possession thereof permanently."[29] At common law, neither services nor labor could be the subject matter of theft since neither could be carried away. Thus, the use of a computer was not something which could be stolen. On the other hand, that which could be carried away, the card decks and printouts found in Lund's possession, had value only as scrap. Even the director of the computer center admitted they were worthless. Thus, what Lund had taken that had value, the use of the computer, could not be stolen, and that which had been stolen had no value. The Supreme Court of Virginia, therefore, struck down Lund's conviction.[30]

This case, like *McGraw*, poses questions about the wisdom of the court's reasoning. Those who have studied and practiced law are realistic enough to believe that judges who serve on appellate courts sometimes reach the decision they find most acceptable to their own inclinations and then work backward to draft an opinion to justify it. It is easy to want to dismiss the charges against Lund since his "illicit" actions were related directly to his graduate work, and would have been "licit" if he had followed the proper procedures. At most, his actions created a minor annoyance for some computer users. But what if Lund had been using VPI's computer for his own private business as McGraw was doing with his employer's computer? Or, what if Lund had been selling computer science programming assignments to freshmen? Would the justices of the Supreme Court of Virginia have found as they did, and would we have been satisfied with their decision? The Virginia legislature responded to *Lund* by amending the Criminal Code to make Lund's activity a crime.[31] Nevertheless, Virginia's supreme court, like Indiana's, took a position that tends to minimize misuse of a computer system in the eyes of the law.[32]

Another case which provoked considerable discussion as to

29. 217 Va. at 693, 232 S.E.2d at 748.

30. *Id.* at 693, 232 S.E.2d at 748-49.

31. VA. CODE ANN. § 18.2-98.1 (1982), *repealed and replaced by* Virginia Computer Crimes Act, VA. CODE ANN. § 18.2-152.1 to -152.14 (Supp. 1987). *See* Evans v. Commonwealth, 226 Va. 292, 308 S.E.2d 126 (1983).

32. The fact that Lund would not have had to serve a prison term even if his conviction had been upheld, 217 Va. at 688, 232 S.E.2d at 746, does not encourage prosecutors to pursue those who have been found to make unauthorized use of a computer system.

whether certain computer abuses should have criminal penalties is *People v. Weg.*[33] Theodore Weg, a computer programmer employed by the Board of Education of the City of New York, used the Board's computer to keep track of the genealogy of race horses. He maintained that he was doing so to learn how to use a data base management program that the Board had recently obained. There were no allegations that he made any money from this unauthorized use of the computer. He was charged with violating a statute which included as theft of services:

> Obtaining or having control over labor in the employ of another person, or of business, commercial or industrial equipment or facilities of another person, knowing that he is not entitled to the use thereof, and with intent to derive a commercial or other substantial benefit for himself or a third person, he uses or diverts to the use of himself or a third person such labor, equipment or facilities.[34]

Judge Juviler reviewed the history of the statute and concluded that, based on the original purpose of the statute and its legislative history, computers were not the industrial equipment or facilities that the lawmakers had in mind. Computers were more in the nature of a service. The lawmakers had specifically refused to include theft of services in a 1967 revision of the penal law since that would have led to hosts of criminal charges of a basically civil nature.

> If "business equipment or facilities" . . . 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, typewriters, and other equipment or facilities for personal benefit. The Legislature could not have intended such a dramatic change in the criminal law . . . transforming "basically civil" wrongs to misdemeanors punishable by a year in jail without giving clearer indication of its novel purpose.
>
> . . . .
>
> In 1982 the Legislature could reasonably find a need to regulate, even by penal sanction, conduct of the type alleged in this information. 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. This court,

33. 113 N.Y. Misc. 2d 1017, 450 N.Y.S.2d 957 (1982), *reprinted in* I Computer L. Ser. Rep. (Callaghan) 478 (N.Y. Crim. Ct. 1982).

34. 450 N.Y.S.2d at 958 (citing N.Y. PENAL LAW § 165.15(8) (McKinney Supp. 1986)).

however, may not create an offense.[35]

Perhaps computers are a "special type of expensive, commonly owned equipment so subject to misuse" that lawmakers should make special provisions to punish misuse that might otherwise be tolerated with respect to less powerful and potentially troublesome tools of industry and government. Courts, like that of Judge Juviler, however, have been reluctant to rewrite the law as they see it.[36]

Computers have given rise to new forms of vandalism that can have serious implications for persons and businesses who depend upon their computers. The October 21, 1985 issue of *Infoworld* carried a story about a Southern California programmer who has been charged with two felony counts of malicious intent to damage a computer system.[37] The charges stemmed from a "logic bomb" that the programmer had allegedly placed in a program he wrote for Creative Peripherals Unlimited.[38] The bomb placed a "worm" inside the user's operating system which counted the number of times the program was run. When a certain number was reached, the worm changed the data disk's identification code so that the user could no longer reach his or her own data.[39]

Another form of computer vandalism is the placement of destructive programs on publicly accessible electronic bulletin boards. These programs are described to the user as performing useful functions, such as a screen dump, but they contain logic bombs. By the time the user realizes the true nature of the program, substantial damage has been done to his data.

There is even the threat of logic bombs placed in commerically available programs that can damage data stored in computer systems

35. *Id.* at 961.

36. *See also* Giss v. Sumrall, 409 So. 2d 1227 (La. App. 1981) (the court rules that an employee who was fired for using the company computer for an area real estate business he operated on the side was entitled to unemployment compensation). A result similar to that in *Lund* was obtained in People v. Home Ins. Co., 197 Colo. 260, 591 P.2d 1036 (1979) (what was "stolen" in this case was confidential medical information).

37. Infoworld, Oct. 21, 1985, at 6, col. 4.

38. A "logic bomb" is code in software whose operation, usually highly destructive, is triggered by the occurrence of some event. In this case the event was running the program in which the bomb was contained a certain number of times. A typical destructive effect is erasing all of the user's data stored on a hard disk.

39. A "worm" consists of instructions which infiltrate the computer's ordinary operating instructions and which interfere, often unpredictably, with that operation. The programmer denied that there were any intentional bugs in the program although he knew that there were some bugs. He believed that these had been corrected. He also stated that Created Peripherals owed him a substantial amount of money and had breached their contract with him. Infoworld, *supra* note 37.

when they detect attempts to copy the program. Such copying might not be an attempt to violate the copyright laws but a legitimate attempt by an honest user to back up a valuable investment. The owner of the legitimate copy might not even be aware that an attempt at copying has been made, but he or she would still have to bear the consequences of the triggered logic bomb.

Should "booby traps" placed in computer systems be the subject of criminal legislation, or should injured parties be allowed a remedy only through civil actions? The threat of civil liability may not be sufficient to deter computer vandals who may have little money with which to pay a judgment. Also, such civil actions are expensive and time-consuming and the requisite evidence difficult for a private party to obtain. A logic bomb placed in a commercially distributed program, or distributed through electronic bulletin boards, is the computer equivalent of deliberately distributing tainted goods which can cause indiscriminate injury to any person unlucky enough to ingest the tainted goods. The economy of the nation cannot tolerate computer terrorists.

The case of Tom Tcimpidis introduces another facet of computer abuse which the law was unable to address adequately.[40] On May 16, 1984, law enforcement officers from the Los Angeles Police Department and employees of Pacific Bell Telephone swooped down on the home of Tcimpidis, served a search warrant on the startled computer hobbyist and electronic bulletin board operator, and carted away computer equipment worth thousands of dollars.[41] The reason for the raid was that earlier in the month, security officers for the telephone company had noticed that an anonymous user had posted one AT&T and two Sprint long-distance codes with instructions to "enjoy." Tcimpidis was charged with telephone fraud, a misdemeanor for which convictions can carry a penalty of up to a year in prison and a $10,000 fine. A lawyer and computer hobbyist, Charles Lindner, agreed to defend Tcimpidis for out-of-pocket expenses alone; and these expenses were to be met by contributions from other outraged computer users.

40. For an excellent account of the Tcimpidis case, see Watt, *Use a Modem - Go to Jail?*, Profiles, February 1985, at 28.

41. An electronic bulletin board system of the type that Tcimpidis operated consists of a hard disk, a modem, a microcomputer, and appropriate software. A user accesses the system by dialing a particular telephone number; the connection is made over a telephone line using the modem. The user is then free to post messages on the bulletin board by creating a new file, or adding to an existing file, on the hard disk. The user can obtain messages from the board by reading files stored on the hard disk.

There is no doubt that someone placed illicit data on Tcimpidis' bulletin board. At the time, the bulletin board was available to anyone who had the telephone number and the necessary equipment. In the approximately four years of operation before the "bust," hundreds of callers had left nearly 100,000 messages. The sheer volume of messages, coupled with the fact that the board was Tcimpidis' hobby and not his livelihood, was almost certain evidence that he had no knowledge of the illicit message which gave the long-distance access codes. It is probably this consideration that finally led the prosecutor to drop the charges, because if Tcimpidis did not know about the presence of the message, he could not have been found guilty.

An interesting aspect of the law under which Tcimpidis was charged is that it did not require proof of any loss on the part of the telephone company or anyone else. It did not even require that the telephone credit card number be real. Anyone could be charged who published

> the number or code of an existing, canceled, revoked, expired or nonexistent credit card, or the numbering or coding which is employed in the issuance of credit cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful telephone or telegraph toll charge.[42]

The Tcimpidis incident raises the question of the extent to which computer system operators should be held accountable for illicit activity conducted on their systems. It also raises constitutional questions concerning the right of free speech. To place severe constraints on those who operate means of communications like electronic bulletin boards, which are becoming increasingly popular as methods of information interchange, risks the proverbial "chilling effect" that may hamper first amendment rights.[43]

The primary issue raised by the selection of cases reviewed in this article is this: What computer-related acts are so dangerous to the public welfare that society should punish, through its system of criminal justice, those who commit them? How seriously should we view attempts by "hackers" to break into the computer systems of hospitals, businesses, and even defense establishments? Many of these security breaches come from inadequate safeguards at the break-in site; at times, employees of the computer operations themselves provide

42. CAL. PENAL CODE § 502.7(c) (West Supp. 1986).

43. A major issue, yet to be settled, is whether computer bulletin boards have the first amendment rights of newspapers, the rights of public broadcasters, or the rights of neither.

the necessary information for compromising the system. To what extent should we punish someone who provides the information needed to commit a crime, knowing that others will then use this information to commit it? There is at least one underground newspaper dedicated to providing information to defraud the phone company.[44]

The Tcimpidis incident raises issues of free speech and open communications. How many controls should the government be permitted to impose on data flow in the name of stifling abuses? To what extent should computer operators be held responsible for illicit activity carried out on their system? Too much government monitoring can easily lead to stifling information flow, and too little can pose a serious threat to the national government with weapons against legitimate dissent, but laws or courts that are too lenient can create an environment that encourages computer thieves to try their luck at will.

Should we punish someone for the unauthorized use of his or her employer's computer? Should the answer to this important question be determined by the activity carried out on the machine, and, if so, what activity should be punished? Is the computer substantially different from the telephone and the hammer as a tool in modern society, and, if so, how does this translate into law?

There is no question that new legislation is needed to address the issues that computer use raises; but, the kind of legislation that would most favor our societal goals is far from obvious. If the law fails to address the issues intelligently now, we may find that we have lost the opportunity to address them at all, later.

44. The newspaper is appropriately named TAPS. Now electronic bulletin boards can serve the same function as underground newspapers, as the Tcimpidis incident illustrates.