LEGAL PROBLEMS OF COMPUTER ABUSE

SUSAN HUBBELL NYCUM*

Computer abuse consists of incidents caused by intentional acts from which a perpetrator realized or could have realized a gain and/or a victim suffered or could have suffered a loss.[1] This paper focuses on the legal problems of computer abuse; the material presented herein is based on a multi-year study supported in part by the National Science Foundation. The study now includes an analysis of over 500 reported incidents of computer abuse (the "case file"). Data concerning the abuses was gathered from sources including the news media; interviews with victims and perpetrators; access to public and private files, including police and auditor investigative reports, arrest and search warrants, charges, trial transcripts, and court opinions. Approximately fifty percent of the case files have been verified by the investigators' personal contact with the participants. Thirty of the cases have been investigated in the field.

As of August 1977, the losses associated with incidents of computer abuse, excluding the Equity Funding fraud of 1973[2] which resulted in losses exceeding $2 billion, were over $100 million. Losses have averaged $5 million per year over an eleven year period and, in the past five years, losses have increased to an average of $10 million per year. Since 1958, the occurrence of reported cases has grown virtually exponentially as a result of the increasing use of computer technology in sensitive areas of activity in both the public and private sectors. Unfor-

---

* Attorney, Chickering and Gregory, San Francisco, California. Ms. Nycum is the co-author of COMPUTERS AND THE LAW (1975), is on the Board of Directors of the Computer Law Association, and is vice-chairperson of the American Bar Association Section on Science and Technology.

1. The terminology was adopted as a term of art in the law by the United States Court of Appeals for the Fourth Circuit. *See* United States v. Jones, 553 F.2d 351 (4th Cir. 1977).

2. In this $2 billion fraud scheme, which was discovered in 1973, the Equity Funding Corporation of America "created" 64,000 bogus insurance policies—by use of the computer—to sell to reinsurers. This computer abuse has resulted in 22 convictions on federal charges and at least 50 major law suits. *See generally* D. PARKER, CRIME BY COMPUTER 118-74 (1976).

tunately, the support functions which made that technology impervious to misuse have not kept pace with the abuse. This security lag has provided the opportunity for injury.

Abuses have been categorized by the study in several ways, but the following are of principal interest: injury to computer hardware and system software; injury to computerized data and applications programs; injury in which the computer was the perpetrating device; injury in which the computer was used as a symbol, *e.g.*, for intimidation or deception.

The category of "inspec" or "nonspec" differentiation separates those incidents in which the computer was used in accordance with proper specifications, but the data inputted or outputted was improperly altered (inspec), from those in which the computer processes themselves were compromised (nonspec). The more sophisticated abuses are in the nonspec category; however, monetary losses to date have resulted more frequently from inspec abuses.

Seventeen perpetrators have been personally interviewed to date. The perpetrators are generally highly intelligent, aggressive, verbal, and eager; in many respects they are desirable employees. Perpetrators are usually young, between eighteen and forty-six years of age, with a mean age of twenty-nine and a median age of twenty-five. They are generally skilled, and managerial and technical skills predominate. Of the seventeen perpetrators, eleven performed their acts from positions of trust and fifty percent of the acts required collusion (in contrast to white collar criminals generally, who work alone eighty-nine percent of the time). While thirteen perpetrators deviated insignificantly from the accepted practices of their associates (the differential association syndrome), twelve perpetrators evidenced the Robin Hood syndrome: they considered harming people to be wrongful, but rationalized harming organizations and particularly computers in organizations. In addition, fifteen perpetrators considered the act an intellectual challenge; they enjoyed pitting their technical skill against the intransigent machine. Eight perpetrators received known financial gain averaging $500,000 per case, with a range of $1,400 to $1,500,000. Their occupations ranged from time-sharing computer service users and business programmers, to presidents of computer-related firms, sales managers, directors of data processing operations within organizations, accountants, bank tellers, and retail consumers.

Disposition of the cases of the seventeen perpetrators was:

Felony conviction	9
Felony charged	1
Civil judgment	1
Charges dropped	1
No action taken	4
Perpetrator hired by the victim	1

Legal aspects of computer abuse are best discussed in the context of the taxonomy of computer abuse itself: acts directed at computers or computer systems; acts directed at computerized assets; acts in which the computer itself is the perpetrating tool or device; and acts in which a computer may or may not be involved but nevertheless is the symbol of the abuse.

In the first category—acts directed at computer equipment—the legal analysis is traditional, because these assets are tangible personal property, and the acts are recognizable under familiar principles of law. The wrongful taking of computers fits conveniently into traditional forms of theft, involving both larceny or outside theft and embezzlement or inside theft. Similarly, capture of a computer and holding it for ransom has legal elements analogous to those of criminal extortion or other crimes comprised of acts against personal property and the ownership or possession thereof.

On the other hand, acts of abuse directed toward computer systems are not easily categorized under the familiar legal concepts applied to tangible personal property. For example, when the computer itself is unharmed, but the software has been altered or destroyed, it is difficult to analyze the act in traditional criminal law terms. A prosecutor may be unable to frame an indictment for malicious mischief, because some malicious mischief statutes, and cases interpreting them, address the damage to or injury of a tangible.[3] When the tangible, in this case the computer, is left unharmed, but the software which enables it to function is compromised, there is no discernible injury to any physical representation.

There are several incidents in the case file where this situation has occurred. In one case, a very sophisticated injury was inflicted upon

3. *See, e.g.*, N.J. STAT. ANN. §§ 2A:122-1, :170-36 (West 1969); 18 PA. CONS. STAT. ANN. § 3304(a) (Purdon 1973); TEX. STAT. ANN., PENAL CODE ANN. tit. 7, § 28.03(a)(1) (Vernon 1974).

a large life insurance company. The company's numerous branch offices collected large amounts of data each day, which was stored on remote terminals. After the close of business, the computer at the central site would automatically poll the various branch offices by activating the remote terminals and causing them to transmit the day's transactions to the central site. A group of perpetrators managed to simulate the electronic impulses which initiated the transfer of the data. Using public telephones, the perpetrators called the branch offices at random, and caused the branch office terminals to attempt to transmit the data. As a result, the computer tapes were unwound and, when the real host computer polled the remote site, the remote terminals were unable to respond. This sabotage resulted in a loss of thousands of dollars to the insurance company, including out-of-pocket expenses for a period of several weeks during which the company and hardware vendor attempted to locate the perpetrators. The perpetrators, it was discovered, were disgruntled Customer Engineers of the computer hardware vendor who serviced the installed hardware at the insurance company.

The significance of this case from a legal standpoint arises from the discovery by the prosecutor, the District Attorney for Westchester County, New York, that a New York statute prohibiting obscene or harassing telephone calls was the only applicable legal sanction. Violation of this statute is a misdemeanor punishable by a fine, which is not fully responsive to the injury incurred.[4] Unfortunately, this incident may not be unique to the insurance industry. The increasing use of point-of-sale devices, which may transmit data in batches after business hours from individual retail outlets to central processing locations or clearing houses in electronic funds transfer systems, presents additional targets for this type of abuse.

The second area of computer abuse is abuse to computerized assets and computer services. These acts include theft of computer time which may not, depending on the jurisdiction's definition of property in the theft statutes, be subject to sanction, even though computer time is a very valuable resource.[5] An early case of abuse to computerized

4. The malicious mischief sanctions and anti-tempering statutes contemplate injury to tangible personalty. For a full discussion of the law of selected states on this point, see Nycum, *The Criminal Law Aspects of Computer Abuse*, 5 RUTGERS J. COMPUTERS & L. 271 (1976).

5. *See, e.g.*, CAL. PENAL CODE § 484 (Deering 1971); DEL. CODE ANN. tit. 11, § 845 (1975); N.Y. PENAL LAW § 165.15(7) (McKinney 1975); 18 PA. CONS. STAT.

assets is *Ward v. Superior Court.*[6] Ward obtained an intangible copy of a proprietary computer program from the computer, where its owner stored it, and caused it to be transferred to Ward's employer's computer. Ward then caused a hard copy of the program to be printed and took that copy. Ward's acts led to the first instance of a computer memory being the subject of a search warrant. The court denied the defendant's motion to dismiss the information charging him with taking a trade secret in violation of the California Penal Code.[7] The judge found that there was probable cause to believe that a taking and carrying away of a trade secret represented by the computer program had been committed. This was the first time a computer program had been characterized as a trade secret under the California Penal Code. The judge, however, also found that the mere transference of the electronic impulses from computer A to computer B did *not* constitute a taking of the trade secret; the crime required Ward's carrying the printed copy to his office to consummate the theft.[8] It is important to note that computer display devices enable a person to see a program, use it, alter it, and never make a copy of the program itself. This loophole in the law is potentially dangerous to software owners.[9]

Because of the deficiencies in the laws discussed above, Senator Ribicoff has introduced S. 1766, the Federal Computer Systems Protection Act of 1977,[10] which would make it a felony (a) to access certain

---

ANN. § 3926 (Purdon 1973); TEX. PENAL CODE ANN. tit. 7, § 31.03 (Vernon 1974 & Supp. 1976-77).

6. 3 Computer L. Serv. Rep. [C.L.S.R.] 206 (Cal. Super. Ct. 1972).

7. CAL. PENAL CODE § 499c (Deering Supp. 1977). Section (b) of the statute provides, in part:

> (b) Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret, or with an intent to appropriate a trade secret to his own use or to the use of another, does any of the following:
>
> (1) Steals, takes, or carries away any article representing a trade secret.
>
> . . . .
>
> (3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.

The company that employed Ward was subsequently found liable in a civil proceeding for unfair competition.

8. The judge found that subdivision (3) of the statute encompassed Ward's crime. 3 C.L.S.R. 206, 209. *See* note 7 *supra.* The court said Ward could also be charged with theft of property under the general theft statute. *Id.* at 210-11.

9. *See, e.g.*, United States v. Bertram Seidlitz, No. 76-079H (D. Md. June 14, 1976).

10. S. 1766, as introduced in the Senate on June 27, 1977, provides:

> SEC. 2. The Congress finds that—

specified computer systems for the purpose of (1) devising or executing a scheme to defraud, or (2) obtaining money, property, or services by false pretenses or representations or promises, and (b) intentionally and

---

(1) computer related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer related crimes in Federal programs, in financial institutions, and in other entities which operate in interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer related crime directed at institutions operating in interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer related crime is difficult under current Federal criminal statutes.

SEC. 3.(a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

§ 1028. Computer fraud

(a) Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, computer network, or any part thereof which, in whole or in part, operates in interstate commerce or is owned by, under contract to, or operated for, on behalf of, or in conjunction with, any financial institution, the United States Government, or any branch, department, or agency thereof, or any entity operating in or affecting interstate commerce, for the purpose of (1) devising or executing any scheme or artifice to defraud, or (2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, shall be fined not more than $50,000, or imprisoned not more than 15 years, or both.

(b) Whoever, intentionally and without authorization, directly or indirectly accesses, alters, damages, or destroys any computer, computer system, or computer network described in subsection (a), or any computer software, program, or data contained in such computer, computer system, or computer network, shall be fined not more than $50,000, or imprisoned not more than 15 years, or both.

(c) For purposes of this section, the term—

(1) 'access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

(2) 'computer' means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

(3) 'computer system' means a set of related, connected or unconnected, computer equipment, devices, and software;

(4) 'computer network' means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(5) 'property' includes, but is not limited to, financial instruments, infor-

without authorization to access, alter, damage, or destroy those computer systems.

The new federal Privacy Act of 1974[11] and the privacy laws of some states[12] address the problem of abuse to another type of computerized asset—personal information. Those laws make it a misdemeanor to wilfully maintain a secret system of records about individuals, for an employee of a government agency wilfully to provide information improperly to organizations or persons, and for an outsider to obtain information which he is not entitled to by means of artifice or

---

mation, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;

(6) 'services' includes, but is not limited to, computer time, data processing, and storage functions;

(7) 'financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security;

(8) 'computer program' means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

(9) 'computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

(10) 'financial situation' means—

(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

(B) a member of the Federal Reserve including any Federal Reserve Bank;

(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

(D) a credit union with accounts insured by the National Credit Union Administration;

(E) a member of the Federal Home Loan Bank Systems and any Home Loan Bank;

(F) a member or business insured by the Securities Investor Protection Corporation; and

(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934.

(c) The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following: "1028 ——— Computer fraud.".

123 CONG. REC. S10,792 (daily ed. June 27, 1977).

11. *See* Privacy Act of 1974, 5 U.S.C. § 552a (Supp. V 1975).

12. Omnibus Privacy legislation has been passed to date in the states of: Arkansas-ARK. STAT. ANN. §§ 16-801 to 16-810 (Supp. 1977); California-Information Practices Act of 1977, ch. 709, 1977 Cal. Adv. Legis. Serv. 549 (to be codified as CAL. CIV. CODE § 1798 (Deering); Connecticut-CONN. GEN. STAT. §§ 4-190 to 4-197 (1977); Indiana-Pub. L. No. 21, 1977 Ind. Acts —; Massachusetts-Mass. ANN. LAWS ch. 66A, §§ 1-3 (Michie/Law. Co-op. Supp. 1977); Minnesota-MINN. STAT. ANN. § 15.165 (West 1977); New Hampshire-N.H. REV. STAT. ANN. §§ 7-A:1 to 7-A:5 (Supp. 1975); Ohio-OHIO REV. CODE ANN. §§ 1347.01-1347.10, 1347.99 (Page Supp. 1976); Utah-UTAH CODE ANN. §§ 63-50-1 to -10 (1977); Virginia-VA. CODE §§ 2.1-377 to -386 (Supp. 1977).

trick. The federal and state laws, which are generally similar, provide sanctions for theft of information from files maintained by government agencies. There is not, however, an existing remedy for carelessness in transferring data, nor a method for insuring that once a system has been compromised, either intentionally or through inadvertence, the data still maintains its integrity. There is no required audit to insure that the information given subsequent to a disruption of the system will be the same data as was recorded in the automated system prior to that disruption. It is suggested that future case law may establish further rights of data subjects whose records are contained in an automated system of records. Recourse to traditional legal principles will raise many of the same issues previously discussed in the context of malicious interference with software or the theft of software and data.

In the third category of abuse, where the computer itself is the perpetrating tool or device, it is generally the targeted act, rather than the means of perpetrating the act, with which the law is concerned. As most of these targeted acts are traditional forms of embezzlement and fraud, they pose little difficulty for the lawyer, judge, or jury. There is a serious problem, of course, for the law enforcement officer who must discover how the acts were perpetrated and how to provide evidence concerning the perpetration. The case file contains many examples of these perpetrations, ranging from very simple ones such as the kindly keypuncher who ignored the names and addresses of friends when typing up the master files for municipal parking violations to the massive $2 billion Equity Funding fraud.[13]

There is a related concern and uncertainty with respect to the responsibilities of auditors. Accountants' legal duties to investigate have recently been expanded and they are cognizant of their extensive potential civil and criminal liability under modern law.[14] At a time when the responsibilities for detecting fraud have increased, the computer has decreased the opportunity to successfully detect fraud. The accountant can no longer be satisfied that he can properly audit the function of an organization by traditional means. Unless he and his colleagues

13. *See* note 2 *supra.*

14. This trend may have been somewhat curtailed by Ernst & Ernst v. Hochfelder, 425 U.S. 185 (1976). The Supreme Court found that liability under Rule 10b-5 for nondisclosure must be predicated upon scienter; negligence is insufficient.

have computer skills, they are at the mercy of an automated record-keeping system. And, even with computer skills, the ability to audit may be limited to inspec abuses.[15]

The fourth area of abuse, in which the computer is used as a symbol, can also be subjected to a traditional legal analysis. The Federal Trade Commission and others are alert to potential abuses by companies which purport to match a customer with his life's dream by a computerized dating service, or companies which purport to make the customer a valuable member of the business community earning well over $12,000 after a two-month course of "hands-on" computer experience at the company computer programming school. More likely than not, the customer does not meet anyone compatible through the dating bureau, which may not even have a computer. Frequently, the computer school does not have a computer on site, but only a terminal; and, instead of becoming a programmer, the customer may be fortunate if he learns how to operate the terminal.

There have been cases in which the computer has been blamed either for loss of information or the use of incorrect information—such as the "computer" loses the record of a life insurance policy, or payment of a bill, or causes a policy to lapse, or a utility to be turned off—and a company has tried to avoid responsibility for it. The courts, however, have seen through the "computer" artifice and concluded that behind the computer was a fallible human being who breached his duty to exercise traditional human intelligence and skills.[16]

---

15. Inspec abuses, where the data inputted or outputted was improperly altered, account for most dollar losses, *see* p. 528 *supra.*

16. *See, e.g.*, Palmer v. Columbia Gas Co., 342 F. Supp. 241 (N.D. Ohio 1972), *aff'd*, 479 F.2d 153 (6th Cir. 1973). Residential natural gas customers sought injunctive and declaratory relief from Columbia Gas Company. The plaintiffs alleged that the company terminated their gas service under color of state law without due process of law. Although the crux of the case was whether the utility company acted under color of state law and whether its termination procedures afforded its customers due process, the court acknowledged the role of defendant's computer in the termination process. The facts showed that estimated bills issued by defendant's computer were often understated. When customers' meters were read, the discrepancies between the computer's estimated charges and the customer's actual charges were often so high that customers could not pay their bills. The issuance of termination notices was also handled by the computer. The computer's role in the process, however, did not prevent the court from granting plaintiffs relief against the defendant company. The district court found that the defendant relied "uncritically upon its computer." *Id.* at 243.

Conclusion

The rapid development of computer technology provides a perpetrator with the capability to commit a wrong for which the present law may have no remedy. Carefully drafted legislation at both the federal and state levels may be the only way to effectively combat crime in a computerized environment. Hopefully, state legislators will consider introducing and supporting legislation similar to that proposed by Senator Ribicoff at the federal level to fill the gaps in state laws.[17]

17. At this writing S. 1766 is not an ideal piece of legislation. The author and others expect to suggest changes to the bill if hearings are scheduled.