U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NATIONAL INSTITUTE OF JUSTICE

Research in Action

Charles B. DeWitt, Director

November 1991

State Computer Crime Statutes

by Hugh Nugent

In late 1988, Robert T. Morris, a Cornell University graduate student, shut down a nationwide computer network with what rapidly became the best known computer worm in history. Prosecuted in Federal court for violation of the Federal computer crime statute, Morris eventually received a fine and probation.[1] But his actions cut loose a torrent of public discussion on the adequacy of the criminal justice system to deal with predators as skillful as but more malicious than Morris.

Computer technology is omnipresent in contemporary American life. We pump gas from computerized pumps; receive computerized bills from public utilities for service that is largely computerized; receive computerized grocery checkout lists, which are part of computerized inventory control systems; take off, fly, and land in planes guided by computers; telephone friends on the other side of the country on computerized telecommunications systems; get telephone calls from computers; read articles, including this one, written on computers.

Hugh Nugent is an attorney and principal associate for the Institute for Law and Justice, Inc., in Alexandria, Virginia.

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Institute for Law and Justice, Inc., under contract number OJP–85–C–006.

State and Federal legislators are fully aware that we have entered the computer age. In the 10 years before the Morris worm, 48 of the 50 State legislatures and the U.S. Congress had passed some form of computer crime statute. Morris probably could have been prosecuted in every State in which his worm entered a computer, for either unauthorized access or computer damage.

When the National Institute of Justice surveyed criminal justice agencies through its National Assessment Program, police chiefs and sheriffs reported a need for more information and research on effective computer crime investigation. As part of its response, NIJ published "Dedicated Computer Crime Units," an *Issues and Practices* report that examined special units that some jurisdictions have established specifically to investigate computer crime. As part of that study, researchers prepared an overview of State statutes on computer crimes.

This *Research in Action* summarizes the results of that effort. It examines the background and the contents of the State computer crime statutes, first with a brief discussion of some underlying issues of judicial construction and then with a review of some of the earlier computer crime cases. This background will give a better understanding of issues legislatures had in mind while drafting their computer crime statutes. The article then examines several features found in the statutes themselves, pointing out how different

From the Director

The past decade witnessed a dramatic rise in the use of computers and increasing reliance upon them throughout society. The benefits of computer technology, and its future potential, are clear. What has also become clear to the law enforcement community is the capacity of the computer as a tool for criminal activity.

Law enforcement is responding to the challenges posed by computer crime with new investigative and prosecutorial methods. The National Institute of Justice has helped with information about how agencies can implement them.

This *Research in Action* shows how State lawmakers have responded to computer crime by enacting statutes specifically targeting illegal computer activity. It summarizes some of the practical considerations that must be grappled with in responding to this criminal justice challenge.

Charles B. DeWitt
Director
National Institute of Justice

States have approached the same problems in different ways.

Strict construction of criminal statutes

The constitutional concept of due process of law, expressed in the 5th and 14th amendments of the U.S. Constitution, requires that everyone be put on clear notice that certain acts are criminal acts. This means that legislatures are to state, in terms understandable by the ordinary person, exactly what they intend to compel or prohibit. This matter of terms is one to which a great deal of attention has been paid in computer crime legislation, but anyone examining the definitions adopted would find it hard to say that they are readily understandable by the ordinary person.

A basic principle of judicial construction is that criminal statutes are strictly construed against the State and in favor of the individual. That is, courts will not interpret a statute liberally or broadly to cover the circumstances of a particular case, as they sometimes do in civil litigation, to achieve what the legislature probably had in mind but failed to express with precision and clarity. Courts will not expand criminal statutes to cover acts the legislature probably would have forbidden had it thought of them. Thus, more often than not, strict construction works for defendants in criminal cases.

Finally, a criminal offense consists of certain specific elements, all of which the prosecutor must prove. For example, larceny under common law was taking and carrying away another's personal goods of any value, with intent to steal them. That definition breaks down into four elements to be proved: (1) taking, (2) carrying away, (3) goods of another, (4) intent to deprive the owner of possession permanently. Larceny was often used as the charge against computer criminals where there was not a computer crime statute. Defenses usually raised included (1) that nothing had been "carried away," the allegedly stolen data or computer program having remained on the computer; or (2) that "property" means only "tangible property," and that electronic impulses are not tangible. These defenses did not prevail often, but computer crime statutes focus prosecution more on the real problem and not on these tangential issues.

Computer crime cases under other criminal statutes

Computer crime was not going unpunished before the recent proliferation of computer crime statutes. Virtually every crime involving computers violates laws other than computer crime laws themselves, and prosecutors successfully prosecuted cases for embezzlement, larceny, fraud, and, in Federal courts, for wire fraud and mail fraud. But there were some problems applying older forms to newer offenses, and specifically designed computer crime statutes should alleviate these problems. Civil litigants also had been successful against computer criminals, and because most State computer crime statutes do not specifically provide for civil relief, civil litigants for the most part will continue to rely on common law or alternative statutory remedies.

Several cases collected in an *American Law Reports* annotation provide a useful background on how prosecutors proceeded before computer crime statutes were in place.[2] Some observations:

- Despite some ingenious defense arguments, most courts and prosecutors had little difficulty applying traditional concepts to computer offenses.
- Federal prosecutors frequently turned to wire fraud and mail fraud charges where State prosecutors would have charged fraud, larceny, or embezzlement.
- Courts sometimes refused to apply traditional definitions to new offenses where there was no readily apparent loss by the victim.

Defenses usually rested on the intangible or incorporeal nature of computer transactions. In a Texas case, the defendant stole 59 computer programs and attempted to sell them to one of his employer's clients for $5 million. One of his defenses was that computer programs are not corporeal property and therefore not subject to theft. The court noted that the Texas Penal Code section under which the case was brought defines "property," as related to the crime of theft, as including "all writings of every description, provided such property possesses any ascertainable value." It had no trouble finding that computer programs fall within the meaning of that provision.[3] The Alabama Supreme Court reached much the same conclusion in a civil case involving theft of computer payroll programs.[4]

The "intangibility" argument was also unavailing for a Federal defendant charged with unauthorized use of property of the United States. He had accessed a NASA computer from his home telephone, using its time and storage capacity for his own business. He argued that computer time and storage capacity are not "property" or "a thing of value" within the meaning of the statute under which he was prosecuted, characterizing them as "mere philosophical concepts as distinguished from interests capable of being construed as property." The court rejected the argument:

> The consumption of its time and the utilization of its capacities seem to the court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be questioned. Thus, the uses of the computer and the product of such uses would appear to the court to be a "thing of value" within the meaning of 18 USC §641, sufficient upon which to predicate a legally sufficient indictment.[5]

A Missouri defendant tried a variation on the intangibility argument.[6] He was charged with stealing by deceit after he used another person's automatic teller card to withdraw $800 in 16 transactions of $50 each over a 9-day period. Defendant argued that the indictment failed to state that he had made any representation at all, let alone a fraudulent representation, and failed to state that the bank had acted in reliance on his representations in parting with the $800. The court rejected this argument, saying it was based on the assumption that the misrepresentation had to have been verbal. Actions suffice, and by his actions defendant represented that he had authority to use the other

person's bank card and code. The court stated:

> Just as the facts here show a misrepresentation by defendant through his conduct, so also the facts clearly show reliance thereon by the bank. The machine was so programmed that no money would be paid out without the insertion of the appropriate card and the corresponding personal identification numbers. When those items were supplied, the response was programmed so as to pay out the money. No difference can be perceived whether the bank gave approval after the presentation of those identification items or whether it programmed its acceptance in advance. In either case, the bank equally relied upon the presentation of the card and personal identification.[7]

Several cases illustrate the ease with which Federal prosecutors turn computer crime into wire fraud or mail fraud. For example, two TWA employees in Pittsburgh worked a fraud on TWA by keeping and then voiding one-way tickets that had been paid for in cash. They would give the travelers boarding passes and credit transaction receipts, which few people would even notice, let alone question. The two kept the actual ticket, reassembled the ticket packet, and sent it to auditing to be canceled. Of course, they kept the cash. Part of this transaction entailed printing the ticket, which was done by computer connected to the TWA mainframe in Kansas City. It was this part of the transaction that turned the matter into a Federal wire fraud, of which the two were convicted.[8]

In another case, a retail merchant in Brooklyn used counterfeit credit cards to defraud VISA and MasterCard on 267 spurious purchases worth over $95,000. Because computerized inquiries to the credit card companies were made on interstate telephone lines, he was found guilty of wire fraud.[9]

A third Federal case was a mail fraud case in which the mailing was a relatively minor part of the offense, which in all other respects was clearly a computer crime. While working for Sperry Univac's applications development center, defendants developed a system which used computers to generate sheet music. In doing so, they used substantial amounts of computer time and storage capacity within the central processing unit of the applications center development, all without Sperry Univac's knowledge or authorization. In collaboration with another corporation, they agreed to develop and market their sheet music system. The other corporation sent promotional materials through the mail, supplying the basis for the mail fraud prosecution.[10]

There are three cases where lack of a computer crime statute defeated prosecution. *Lund* v. *Commonwealth*[11] led directly to enactment of Virginia's computer crime statute. It is a good example of a court's refusal to stretch old concepts to fit new offenses. Lund was a graduate student in statistics at Virginia Tech who used the university's computer time and services to work on his doctoral thesis, charging the costs back to various departments. He was prosecuted for grand larceny and larceny by false pretense. The Supreme Court of Virginia reversed his conviction. Strictly construing Virginia's larceny statutes, the court held that computer time and services were not goods and chattels (personal property) within the meaning of the statutes, and they could not be carried away. The Virginia General Assembly responded first by amending the larceny statute to include computer time or services,[12] later by enacting a comprehensive computer crime statute.[13]

In *People* v. *Weg*,[14] defendant was a computer programmer for the New York City Board of Education. He was accused of using the board's computer system to record and retrieve data for his own commercial benefit. More specifically, he was charged with theft of services under New York Penal Code §165.15(8), which reads:

> Obtaining or having control...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 deprive 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.

The court held that the board of education's computer was not "business" equipment, since both the statutory context and legislative history clearly indicated that the legislature had meant to protect equipment in commercial use. The board's computer service was not rented or sold to outsiders for a fee.

The court went on to point out that if the legislature wanted to make unauthorized use of computers a crime, it could do so, as Illinois had done:

> This Court, however, may not create an offense. Unless Penal Law section 165.15(8) is amended, it will apply only to unauthorized tapping into a computer whose service is for hire.[15]

Finally, in *State* v. *McGraw*,[16] McGraw worked for the city of Indianapolis as a computer operator. The city leased computer services on a fixed charge or flat rate basis, so its costs did not vary with the amount of use. McGraw was provided a terminal at his desk and was assigned a portion of the computer's information storage area, called a "private library," for his use in performing his duties.

McGraw became involved in a private sales venture and began soliciting his fellow employees and using a small portion of his assigned library to maintain records. Reprimanded several times for selling his products in the office and on office time, he was eventually fired. After he was fired, McGraw asked a former fellow employee to obtain a printout of his business data and then to erase it from what had been his library. Instead, the printout was turned over to McGraw's former supervisor and became the basis for the criminal charges against him.

McGraw was charged with theft, in that he knowingly exerted "unauthorized control over the property of the City of Indianapolis, Indiana, to wit: the use of computers and computer services with intent to deprive the City of Indianapolis..." The Indiana Supreme Court reversed McGraw's conviction because

an element of the offense was missing. The court assumed that McGraw's use of the computer was unauthorized and that such use was "property" under the theft statute. But there was still the question of "deprivation." The quote is presented at length because of the down-to-earth analogies used by the defendant and the court:

> ...Our question is, "Who was deprived of what?"
>
> Not only was there no evidence that the City was ever deprived of any part of the value or the use of the computer by reason of Defendant's conduct, the uncontradicted evidence was to the contrary. The computer was utilized for City business by means of terminals assigned to various employee-operators, including Defendant. The computer processed the data from the various terminals simultaneously, and the limit of its capacity was never reached or likely to have been. The computer service was leased to the City at a fixed charge, and the tapes or discs upon which the imparted data was stored were erasable and reusable. 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. He did not, for his own benefit, withdraw City data intended for its exclusive use or for sale. Thus, Defendant did not deprive the City of the "use of computers and computer services" as the information alleged that he intended to do. We find no distinction between Defendant's use of the City's computer and the use, by a mechanic, of the employer's hammer or a stenographer's use of the employer's typewriter for other than the employer's purpose. Under traditional concepts, the transgression is in the nature of a trespass, a civil matter—and a de minimis one, at that. Defendant has likened his conduct to the use of an employer's empty bookshelf, for the temporary storage of one's personal items, and to the use of an employer's telephone facilities for toll-free calls. The analogies appear to us to be appropriate.[17]

One judge dissented, disagreeing with the majority's conclusion that McGraw did not intend to deprive the city of any property.

> Time and use are at the very core of the value of a computer system. To say that only the information stored in the computer plus the tapes and discs and perhaps the machinery involved in the computer system, are the only elements that can be measured as the value or the property feature of that system, is incorrect.
>
> The fact is the City owned the computer system and all the stations including the defendant's. The time and use of that equipment at that station belonged to the City.[18]

The *Lund*, *Weg*, and *McGraw* cases would all have had different outcomes under computer crime statutes. The court in *Weg* expressly said that the New York Legislature could make computer abuse a crime if it chose to, but that it had not so chosen. The Virginia Legislature reacted to *Lund* in exactly that way, enacting a computer crime statute.

There is another common thread in these three cases. The courts could well have been resisting imposition of severe penalties in cases where victims had not in fact suffered demonstrable monetary loss. In the discussion of computer crime statutes that follows, access without harm is criminalized, although penalties for simple access are usually not harsh.

Computer crime statutes

The first State computer crime statute was enacted in Florida in 1978. It became effective on August 1, 1978, and Arizona's statute took effect 2 months later. Other States soon followed, with 49 now having adopted some form or other of computer crime law. West Virginia and Maine are the most recent, in 1989 and 1990. As this article is being prepared for publication, Massachusetts is in the final stages of enacting a comprehensive computer crime statute, replacing what had been a reference to "electronically stored data" in its general larceny statute.[19] Only Vermont has not enacted specific computer crime provisions.

Except in Virginia, it was not unsuccessful prosecutions under traditional criminal statutes that stimulated this legislative activity. It is hard to say what did, aside from widespread publicity about potential problems. A very interesting analysis of the history of this legislation can be found in an article by Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws."[20]

Most States that have addressed the issue of computer crime have done so in a comprehensive statute, often an independent title in the State criminal code called the Computer Crime Act.[21] At the other extreme, Ohio has inserted a series of computer crime definitions in its general theft statute and added one section on denying access to a computer.[22]

As mentioned above, most States have created a separate code section for computer crime, but many have placed it in other categories such as crimes against property, fraud, theft, or business and commercial offenses. Arizona has placed its computer crime provisions under organized crime and fraud, and North Dakota under racketeer-influenced and corrupt organizations (RICO).

The differences between freestanding computer crime statutes and amendments to existing criminal codes should not be overstated. Some of the former are very brief, targeting computer problems, such as unauthorized access or damage to a computer, and leaving other crimes involving computers to be covered by the criminal code as before.[23] On the other hand, California's computer crime provisions, which appear under crimes against property, are quite comprehensive.[24]

There is a philosophical difference between the two approaches that deserves comment.[25] With the comprehensive approach, the State legislature creates a new set of definitions and offenses, trying to face the broad array of potential criminal opportunities created by com-

puter technology. There is always a fear that new definitions will give rise to new litigation as courts and litigants shake them down into accepted forms.

The other philosophy is to modify existing law by incorporating new concepts within established forms, thereby minimizing the potential for frustrating the legislative will. Established statutory definitions, approved jury instructions, and judicial precedents can be used. For example, if computer crime is viewed as a form of property crime, then the familiar concepts of property crime can be used in developing and defending cases. The impact of change is alleviated.

Although there is no universally recognized model for computer crime statutes, many provisions appear with only slight changes in several States. The typical computer crime statute will contain the following elements:

- Definitions of terms.
- Offenses.
- Elements of offenses.
- Penalties.

Some statutes contain additional provisions:

- Venue.
- Civil remedies.
- Affirmative defenses.

[A compilation of State computer crime statutes as of June 30, 1990, is available on loan from the National Criminal Justice Reference Service (NCJRS), Box 6000, Rockville, MD 20850. Phone 800–851–3420; in Maryland and the Washington, D.C., metropolitan area phone 301–251–5500. Refer to NCJ 127854 when requesting this information from NCJRS.]

Definitions of terms

The definitions set forth in these statutes are always a clear indicator of what problems the legislature is attempting to address. Typically, the following terms will be defined:

- Access.
- Computer.
- Computer network.
- Computer program.
- Computer software.
- Computer system.
- Data.
- Financial instrument.
- Property.

All of the above terms are defined in at least 20 State statutes, and most in over

Definitions Used in the Tennessee Code

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

(2) "Computer" means a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job;

(3) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them;

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data;

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network;

(6) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(7) "Data" is a representation of information, knowledge, facts, concepts, or instructions that are being prepared or have been prepared in a formalized manner, and are intended to be stored or processed, or are being stored or processed, or have been stored or processed, in a computer, computer system, or computer network;

(8) "Financial instruments" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, or marketable security, or any computer system representation thereof;

(9) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(10) "To process" is to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(11) "Property" includes, but is not limited to, intellectual property, financial instruments, data, computer programs, documentation associated with data, computers, computer systems and computer programs, all in machine-readable or human-readable form, and any tangible or intangible item of value; and

(12) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer programs, or data to perform tasks.

30. At the other extreme are several terms that appear in only one or two statutes:

- Computer control language (Maryland).
- Computer data base (Maryland).
- Computer hacking (South Carolina).
- Computer supplies (Wisconsin).
- Data base (New Jersey, Pennsylvania).
- Private personal data (Connecticut, Delaware).
- Supporting documentation (Wisconsin).

These definitions are generally an interesting combination of legal and computer technical styles. Lawyerly words and phrases abound: "including but not limited to," "and any other," "or otherwise," "tangible or intangible," "representation." Computer terms are represented by words like "input," "output," "software," "data base," "supporting documentation," "computer network," "computer system."

To illustrate what State legislatures have been doing with definitions, set forth in the accompanying sidebar are Tennessee's definitions, which are typical.[26]

Several other definitions are of particular interest. For example, according to South Carolina:[27]

> (j) "Computer hacking" means accessing all or part of a computer, computer system, or a computer network for the purpose of establishing contact only without the intent to defraud or commit any other crime after such contact is established and without the use of computer-related services except such services as may be incidental to establishing contact.

In a parallel provision, South Carolina makes computer hacking a computer crime in the third degree, a misdemeanor with a maximum $200 fine and 30 days jail for the first offense, but a felony with a maximum $2,000 fine and 2 years for the second offense.[28] California has a similar provision, but it increases the fine to $5,000 for a second hacking offense.[29]

In its first computer crime statute, Illinois defined "electronic bulletin board" and "identification codes/password systems,"[30] but those terms disappeared in a 1987 revision in favor of the terms most frequently seen in the codes of other States, such as "access," "computer," "computer program," and "data."[31]

Offenses

State statutes do not always give computer offenses specific names and they use a variety of descriptions to state exactly what they are prohibiting. Among the most frequently used titles or descriptions of offenses are the following:

- Access To Defraud.
- Access To Obtain Money.
- Computer Fraud.
- Offenses Against Computer Users.
- Offenses Against Intellectual Property.
- Offenses Against Computer Equipment and Supplies.
- Unauthorized Access.
- Unauthorized or Unlawful Computer Use.

Defining access offenses is a legislative means of applying common law trespass concepts to computers. In other words, an access offense is usually entering someone else's property. If there is no criminal intent beyond curiosity or mischief, then the offense is like South Carolina's definition of computer hacking. But if there is criminal intent, usually to commit a fraud or theft of some kind, then the perpetrator can be prosecuted for both the unauthorized access and the other crime.

There are further wrinkles to access provisions. It is usually specified that interfering with someone else's legitimate access is an offense. Defendants often start out with a right to access, and some States provide for an affirmative defense of authorization, or at least a reasonable belief that access was authorized. Virginia, in a section protecting privacy, draws a line between authorized and unauthorized access, a line that might be easily crossed in an authorized user's search of a data base:

> A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.[32]

Unauthorized access is like trespass. Unauthorized taking of computer programs or data is like theft of any other property. In New York, possession of stolen computer programs or data is, in one sense, like possession of any other stolen property, but, in another sense, like possession of a stolen key or a combination to a safe. Unlawful duplication of computer-related material is a felony. Possession of such material, with the intention to benefit someone other than the owner, is a separate felony.[33]

Elements of computer crimes

State legislatures have drafted their statutes in very similar, although not identical, ways, so a few examples will suffice to show what specific elements they have included in computer crimes. Virginia provides a compact example of a statute that covers many points in four relatively short sections:[34]

> **§ 18.2–152.3. Computer Fraud.** Any person who uses a computer or computer network without authority and with the intent to: (1) Obtain property or services by false pretenses; (2) Embezzle or commit larceny; or (3) Convert the property of another shall be guilty of the crime of computer fraud...
>
> **§ 18.2–152.4. Computer Trespass.** Any person who uses a computer or

computer network without authority and with the intent to: (1) Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network; (2) Cause a computer to malfunction regardless of how long the malfunction persists; (3) Alter or erase any computer data, computer programs or computer software; (4) Effect the creation or alteration of a financial instrument or of an electronic transfer of funds; (5) Cause physical injury to the property of another; or (6) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network shall be guilty of the crime of computer trespass...

§ 18.2–152.6. Theft of Computer Services. Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services...

§ 18.2–152.7. Personal Trespass by Computer. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.

(Another portion of the Virginia statute, Invasion of Privacy, appears in the previous section.[35])

Virginia uses the term "use" where most other States would say "access." Tennessee provides a typical example of how legislatures have specified the elements of access offenses:[36]

(a) Whoever knowingly and willfully, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises violates this subsection and is subject to the penalties of Section 39–14–105.

(b) Whoever intentionally and without authorization, directly or indirectly

(1) Accesses, or

(2) Alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network, or computer software, program or data violates this subsection.

(e) Whoever receives, conceals, or uses, or aids another in receiving, concealing or using any proceeds resulting from a violation of either subsection (a) or (b)(2) of this section, knowing same to be the proceeds of such violation, or whoever receives, conceals, or uses, or aids another in receiving, concealing or using, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing same to have been used in violating either subsection (a) or (b)(2) of this section violates this subsection and shall be subject to the penalties of Section 39–14–105.

Wisconsin exemplifies another approach, that of focusing completely on the computer without reference to intent to commit some other crime:[37]

(2) Offenses against computer data and programs.

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies data, computer programs or supporting documentation.

2. Destroys data, computer programs or supporting documentation.

3. Accesses data, computer programs or supporting documentation.

4. Takes possession of data, computer programs or supporting documentation.

5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(3) Offenses against computers, computer equipment or supplies.

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

A widely publicized computer crime case, *State of Texas* v. *Burleson*,[38] was brought under the Texas provision on harmful access. Three weeks before he was fired by an insurance agency, Burleson had created a logic bomb in the company's systems that would periodically destroy records. Three days after he was fired, the company's computer system suffered a major loss of records, over 160,000 records in three different files.[39] He was tried and convicted under the harmful access section, which reads as follows:[40]

Harmful access

(a) A person commits an offense if the person intentionally or knowingly:

(1) causes a computer to malfunction or interrupts the operation of a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer; or

(2) alters, damages, or destroys data or a computer program stored or maintained, or produced by a computer, without the effective consent of the owner or licensee of the data or computer program.

Penalties

Sanctions provided in State computer crime statutes fall roughly into three classes, each of them used by about a third of the States. The overall sanction system of a State's criminal code is of great importance. A third of the States group all sanctions in a separate part of the code, working towards uniformity in sentencing through a systematic classification of crimes and sanctions. In these States, computer crimes will be classified as Class A Felonies, Class B Felonies, Class C Felonies, Class A Misdemeanors, etc. In such States, the range of penalties and fines will not appear in the computer crime statute itself.

In another third of the States, the penalties are explicitly stated in the computer crime statute. The ranges of fines and sentences are set forth and tied directly to the offenses defined by the statute. Under both these systems, States are penalizing computer crimes at both felony and misdemeanor level. In most States, the maximum penalties will be 5 years and $25,000, but in Nevada, the fine can be $100,000 and the sentence 6 years, and in South Carolina, the fine can be $125,000 and the sentence 10 years.

The third class of computer crime penalties takes a different, and sometimes problematic, approach. It ties the penalty to the amount of damage or loss suffered by the victim. New Mexico sets five levels of sanctions for computer fraud, computer abuse, and unauthorized computer use, depending on the value of the money, property, or services lost:

- Less than $100, petty misdemeanor.
- Between $100 and $250, misdemeanor.
- Between $250 and $2,500, fourth degree felony.
- Between $2,500 and $20,000, third degree felony.
- More than $20,000, second degree felony.[41]

However, such damages are often difficult to measure. Computer services and computer time are bought and sold daily, so arriving at their value should not be difficult. But for proprietary computer uses that are not sold as such, assessing value gets more complex. In a case involving theft of seismic computer programs used in the petroleum industry, an expert witness testified that these programs were worth more than $50, the statutory minimum required to be proved in the case. He also testified that these programs were worth perhaps as much as $2 1/2 million.[42] The statutory minimum obviously had no relationship to the true value of the programs.

In *State of Texas* v. *Burleson*,[43] the insurance company whose records Burleson had destroyed offered evidence on what it cost to replace and rehabilitate those records.

Connecticut and Delaware empower the court, in lieu of imposing a fine, to sentence the defendant to pay an amount not to exceed double the amount of defendant's gain from the offense. The court may hold a separate hearing on that issue if there is insufficient evidence in the record upon which to base a finding of the defendant's gain.[44] Montana sets the ceiling on a fine at two and one-half times the value of the property used, altered, destroyed, or obtained.[45]

Illinois and California have stringent forfeiture provisions, enabling courts to deprive offenders of the instrumentalities of their crimes.[46] The Illinois statute also reaches the fruits or proceeds of the crime.

Wisconsin empowers a sentencing judge, in addition to other penalties, to place restrictions on the offender's use of computers. The duration of such a restriction may not exceed the length of time to which the offender could have been sentenced.[47]

Wisconsin is also one of the States that makes special provision for offenses that create "unreasonable risk and high probability of death or great bodily harm to another," making such offenses Class C felonies.[48] Virginia makes "personal trespass by computer," that is, unauthorized use with intent to cause physical injury, a Class 3 felony.[49]

Delaware classifies offenses creating "a risk of serious physical injury to another" Class C felonies.[50]

Florida makes offenses against computer equipment or supplies a felony of the second degree "if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service..."[51]

Venue

A dozen States include specific venue provisions in their computer crime statutes. Venue refers to the place, that is, the judicial district, in which a case can be prosecuted, which for most crimes is the place where the crime was committed. Venue questions have arisen in computer crime cases because the perpetrator can be at a place quite remote from the place, or places, at which his offense has impact. In a case in which defendants had rigged the Pennsylvania lottery, the offense had impact everywhere in the State where there was a terminal connected to the lottery (1,400 in all). Some of the defendants challenged their prosecution in Harrisburg, claiming that none of the acts that were the basis for the charges had taken place there. The court found from the evidence that the lottery's central computer, without which the rigging could not have taken place, was in Harrisburg and therefore that the offense was committed there.[52]

Venue statutes deal with these problems by making offenses prosecutable in any one of several places. Georgia and Virginia have added provisions pertaining to the computer owner's principal place of business. Georgia's venue provision reads as follows:[53]

> For the purpose of venue under this article, any violation of this article shall be considered to have been committed:
>
> (1) In any county in which any act was performed in furtherance of any transaction which violated this article;
>
> (2) In the county of the principal place of business in this State of the owner or

lessee of a computer, computer system, computer network, or any part thereof;

(3) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, or other material or objects which were used in furtherance of the violation; and

(4) In any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

Civil remedies

Computer crime statutes routinely provide that they are not meant to limit any other provision of civil or criminal codes, leaving the State free to prosecute offenders on other statutory bases, such as fraud or embezzlement, and leaving victims free to pursue their ordinary civil remedies, such as fraud or conversion. Because the level of proof in civil litigation is not as high, and because statutory and common law civil remedies can be broadly construed and shaped to accord relief, there is not the same sense of urgency about providing specific statutory civil remedies for computer crime. But several States have provided such remedies, and it is interesting to note what they have added.

California and Missouri provide compensatory damages, "including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."[54] The same section of the California Penal Code also provides that "the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor."

Other than the compensatory damage language quoted in the preceding paragraph, civil remedy provisions of computer crime statutes do not say much about how the plaintiff's damages are to be measured. Virginia, however, provides that: "Without limiting the generality of the term, 'damages' shall include loss of profits."[55]

Delaware and Wisconsin provide for injunctions against computer offenses as part of their civil remedies. Wisconsin's statute adds protection against bulletin board activity or other disclosure of confidential passwords or codes:

> In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.[56]

California, Illinois, Missouri, and New Jersey provide for attorneys' fees. New Jersey allows the award of punitive damages. Delaware has what amounts to a civil forfeiture provision.[57]

Miscellaneous features

In addition to features common to the majority of computer crime statutes, there are several that appear in only one or two States, but are worth noting. For example, North Carolina has an explicit provision covering extortion:

> Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14–455 [Damaging computers and related materials] with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony.[58]

Georgia and Utah create a statutory duty to report computer crimes to law enforcement officials. Georgia's is the more elaborate of the two:

> It is the duty of every business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corporation; or other business entity which has reasonable grounds to believe that a violation of this article has been committed to report promptly the suspected violation to law enforcement authorities. When acting in good faith, such business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corporation; or other business entity shall be immune from any civil liability for such reporting.[59]

Neither Georgia nor Utah provides any sanction for failure to report. It is not clear that these acts create any greater obligation than citizens already have to report crimes.

Washington makes explicit what is left implicit in most other places:

> A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.[60]

To the extent that other States address this issue, they do so by providing that computer crime provisions are not exclusive and that all other parts of the State code still apply.

In addition to prohibiting unauthorized access to a computer, computer system, or computer network for illicit purposes, Utah makes it a separate offense to allow another person to do the same acts.[61] Iowa addresses a problem about which most other States remain silent, that of proving what is in a computer. The following provision makes printouts admissible as evidence:

> In a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary.[62]

The rule of evidence to the contrary would be the "best evidence rule," that the best evidence of the content of a document is the document itself. Iowa's

statute eliminates any contention that the printout is only a copy of what is in the computer, not the data that are really there. Best evidence rule arguments have been made in earlier cases.[63]

Virginia and West Virginia specifically provide that a computer can be used as an instrument of forgery,[64] legislatively resolving a definitional problem that had vexed at least two Federal courts.[65]

One final note. Oklahoma's statute, reflecting one of that State's principal concerns, includes "geophysical data or the interpretation of that data" in its definition of "property."[66]

Computer worms and viruses

The beginning of this article referred to the computer worm used by Robert Morris to penetrate a national network. Even though most States already had computer crime statutes, several State legislatures amended their statutes to include detailed descriptions of Morris' techniques.

The Morris worm was an independent program that penetrated computers on the network and replicated itself, rapidly overloading the individual computers, first making them sluggish and then causing them to crash. The worm created temporary files that disappeared when the affected computers were shut down, and it did not steal information or destroy files. In the jargon of the industry, because Morris' program was an independent program, it was a "worm." A computer "virus" is a piece of computer code attached to another program.

California's amendment, which refers to both worms and viruses under the rubric "computer contaminant," is illustrative of the new provisions adopted after the Morris incident:[67]

> (10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

Maine and Texas both added "computer virus" to their definitions,[68] and Minnesota added "destructive computer program" to its definitions.[69] Illinois put its new prohibition under "computer tampering."[70]

Conclusion

Justice Holmes considered the States laboratories for working out a variety of approaches to problems confronting our society. The computer crime statutes just discussed are an excellent example of what he was talking about. In a very short period of time, short, that is, as far as lawmaking goes, almost all States have adopted legislation dealing directly and explicitly with computer crime. They have chosen to add these statutes to existing law, rather than to substitute them for prior criminal prohibitions and civil remedies, broadening the options available to prosecutors and civil litigants.

These laws are detailed in definition and comprehensive in scope. But if anything characterizes the criminals at whom these laws are aimed, it is their own ingenuity in finding cracks and loopholes in computer systems and networks. The next decade will provide a test of the strength and precision of these computer laws.

Endnotes

1. Morris was prosecuted under 18 U.S.C. §1030. See *New York Times*, Sec. 1, p. 1, May 5, 1990; *Washington Post*, p. A–1, May 5, 1990, for full discussions of Morris' offense and sentence. An excellent discussion of the Morris worm, its impact, and the prosecutorial issues can be found in Harold L. Burstyn, "RTM and the Worm That Ate Internet," *Harvard Magazine*, p. 23, May–June 1990.

2. *State* v. *McGraw*, 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985), ANNOTATION: Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 A.L.R.4th 971. This is a collection of cases that have been published in case reporting systems, primarily the regional reporters of the West Publishing Company. There undoubtedly have been many other cases, including prosecutions under computer crime statutes, in which there was no reported opinion of the court. E.g., the Robert Morris case is unreported, Morris having pled guilty and there being no written opinion by the court.

3. *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).

4. *National Surety Corp.* v. *Applied Systems*, 418 So.2d 847 (Ala. 1982).

5. *United States* v. *Sampson*, 6 Comp.L.Serv.Rep. 879 (N.D.Cal. 1978).

6. *State* v. *Hamm*, 569 S.W.2d 289 (Mo.App. 1978).

7. 569 S.W.2d at 291 (Mo.App. 1978).

8. *United States* v. *Giovengo*, 637 F.2d 941 (3d Cir. 1980), cert. den., 450 U.S. 1032, 101 S.Ct. 1743, 68 L.Ed.2d 228.

9. *United States* v. *Muni*, 668 F.2d 87 (2d Cir. 1981).

10. *United States* v. *Kelly*, 507 F.Supp. 495 (E.D.Pa. 1981).

11. 217 Va. 688, 232 S.E.2d 745 (1977).

12. See *Evans* v. *Commonwealth*, 226 Va. 292, 308 S.E.2d 126 (1983).

13. Va. Code §§18.2–152.1 through 18.2–152.14.

14. 113 Misc.2d 1017, 450 N.Y.S.2d 957 (N.Y.City Crim. Ct. 1982).

15. 450 N.Y.S.2d at 961.

16. 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985).

17. 480 N.E.2d at 554.

18. 480 N.E.2d at 555.

19. M.G.L.A. c. 266, §30(2).

20. *Criminology*, 26:101, 1988.

21. E.g., see Alabama Computer Crime Act, Ala. Code §§13–A–8–100 through 103; Florida Computer Crimes Act, Fla. Stat. §§815.01 through 815.07; Illinois Computer Crime Prevention Law, Ill. Rev. Stat., ch. 38, §§16D–1 through 16D–7.

22. Ohio Rev. Code Ann. §§2901.01, 2913.81.

23. E.g., see Ala. Code §§102, 103; Ky. Rev. Stat. §§434.840 through 434.860.

24. Cal. Penal Code. §§502, 502.01; see also §§1203.047, 2702.

25. This point was emphasized to the author by a senior deputy prosecuting attorney from the State of Washington, who participated in writing his State's computer crime provisions, which he referred to as one of the "modification" statutes.

26. Tenn. Code §39–14–601.

27. S.C. Code §16–16–10 (j).

28. S.C. Code §16–16–20 (4).

29. Cal. Penal Code §502 (d)(3)(A), (B).

30. Ill. Rev. Stat., c. 38, §16–9, repealed, P.A. 85–926, eff. Dec.1,1987.

31. Ill. Rev. Stat., ch. 38, §16D–2.

32. Va. Code §18.2–152.5, A.

33. N.Y. Penal Code §§156.30, 156.35.

34. Va. Code §§18.2–152–3, 152–4, 152–6, and 152.7.

35. Va. Code §18.2–152.5. See text at note 32, supra.

36. Tenn. Code §39–14–602.

37. Wis. Stat. §943.70.

38. No. 0274120R, Tarrant County, Texas, Criminal Court, 1988.

39. For a discussion of the Burleson case and its investigation, see J. Thomas McEwen, "Dedicated Computer Crime Units," NIJ *Issues and Practices*, 1989.

40. Tex. Penal Code §33.03.

41. N.M. Stat. 30–45–3, 30–45–4, 30–45–5.

42. *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. 1966).

43. See text at note 38, supra.

44. 1984 Conn. Gen. Stat. Ann. §53a–257; Del. Code Ann. Title 11, §937 (f).

45. Mont. Code Ann. §45–6–311 (c)(2).

46. Ill. Rev. Stat., ch. 38, §16D–6; Cal. Penal Code, §502 (g), 502.01.

47. Wis. Stat. §943.70 (4).

48. Wis. Stat. §943.70 (2)(b)(4), (3)(b)(4).

49. Va. Code §18.2–152.7.

50. Del. Code Ann. Title 11, §937 (c).

51. Fla. Stat. §815.05 (2)(b)(3).

52. *Com.* v. *Katsafanas*, 464 A.2d 1270 (Pa. Super. 1983).

53. Ga. Code §16–9–94.

54. California Penal Code §502 (e)(1); Missouri Code §537.525 is almost identical in its wording.

55. Va. Code §18.2–152.12.

56. Wis. Code §943.70 (5).

57. Del. Code Title 11, §939 (a).

58. N.C. Gen. Stat. §14–457.

59. Ga. Code §16–9–95. Cf. Utah Code §76–6–705.

60. Wash. Rev. Ann. Code §9A.52.130.

61. Utah Code Ann. §76–6–703 (3).

62. Iowa Code Ann. §716A.16.

63. See *Hancock* v. *State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).

64. Va. Code §18.2–152.14; W.Va. Code §61–3C–15.

65. *United States* v. *Jones*, 553 F.2d 351 (4th Cir. 1977), cert. den., 431 U.S. 968, 97 S.Ct. 2928, 53 L.Ed.2d 1064.

66. Okla. Stat. Ann. §1952 (8).

67. Ca. Penal Code §502 (b)(10).

68. MRSA §431 (9); Tex. Penal Code §33.01 (9).

69. Minn. Stat. §609.87. Subd. 12.

70. Ill. Rev. Stat. Ch. 38, §16D–3 (4).

For More Information

Computer crime poses unique challenges to law enforcement. The National Institute of Justice moved quickly to provide information resources for handling the investigation and prosecution of computer-related crime.

Computer Crime: Criminal Justice Resource Manual (NCJ 118214) is a comprehensive reference tool covering computer crime.

Organizing for Computer Crime Investigation and Prosecution (NCJ 118216) looks at existing approaches being used by law enforcement, provides specific case examples, and makes recommendations for effective investigation and prosecution of computer crime.

Dedicated Computer Crime Units (NCJ 118215) examines special investigative units set up by local jurisdictions to handle computer crime cases, with staff devoting most of their time to the investigation of computer-related crime.

Write or call the National Criminal Justice Reference Service (NCJRS) for information on obtaining these documents, or for other information on computer crime.

National Institute of Justice/NCJRS
Box 6000
Rockville, MD 20850
800–851–3420
(In Metropolitan Washington, D.C., and Maryland, dial 301–251–5500).

The Assistant Attorney General, Office of Justice Programs, establishes the policies and priorities, and manages and coordinates the activities of the Bureau of Justice Assistance, Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

NCJ 128780

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531

Official Business
Penalty for Private Use $300

BULK RATE
POSTAGE & FEES PAID
DOJ/NIJ
Permit No. G–91