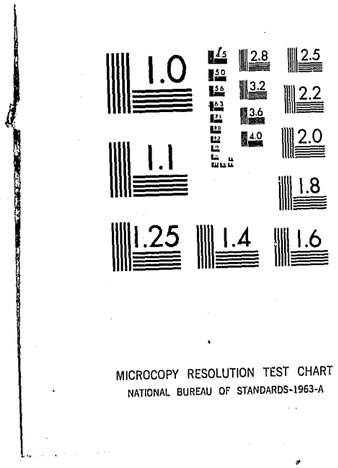

U.S. Department of Justice
Bureau of Justice Statistics

COMPUTER CRIME

Legislative Resource Manual

U.S. Department of Justice
Bureau of Justice Statistics

Benjamine H. Renshaw
Acting Director

Carol G. Kaplan
Director,
Privacy & Security Staff

U.S. Department of Justice
Bureau of Justice Statistics

Computer Crime

Legislative Resource Manual

This document was prepared for the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ) by Koba Associates, Inc. under Contract No. J-LEAA-007-80. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of BJS, DOJ or Koba Associates, Inc.

FOREWORD

In recent years, the problem of computer related crime has confronted our criminal justice system. As criminal elements have kept pace with dramatic technological advances, criminal justice personnel have been forced to become familiar with not only the technical issues associated with computer related crime, but with innovative and effective means of applying legal concepts developed in an era preceding the advent of the first generation of computers.

The Legislative Resource Manual is intended as a background document for criminal justice personnel involved in computer related crime cases. We are hopeful that the Manual will serve to answer many of your fundamental questions regarding the body of law dealing with computer related crime.

Benjamin H. Renshaw
Acting Director
Bureau of Justice Statistics

INTRODUCTION

Over the past quarter of a century our society has witnessed an amazing technological transformation. The computer has become an integral part of our everyday lives, critical to our national defense, financial transactions, and information transmissions. In recent years, the subject of computer related crime has captured the attention of law enforcement personnel, criminologists, the media, and the general public. While our society has been readily afforded access to computer technology so as to improve the standard of living of law-abiding citizens, so too have criminal elements gained access to computers in order to perpetrate illegalities. It has been the realization that criminals possess the capability to access and control high technology processes vital to our everyday lives which has spurred the recent alarm over the issue of computer related crime.

As computer technologies and the means for abusing them have rapidly emerged, they have been confronted by a criminal justice system which is largely uninformed concerning the technical aspects of computerization, and bound by traditional legal machinery which in many cases may be ineffective against unconventional criminal operations. While there is widespread debate as to whether or not laws specific to computer crime are needed, there is general agreement that criminal justice practitioners are at present in need of guidance regarding the conduct of computer related crime investigations and prosecutions. The Legislative Resource Manual is designed to assist criminal justice personnel by familiarizing them with the technical and legal issues confronting computer related crime prosecutions.

The Legislative Resource Manual consists of four major chapters and a series of appendices. Chapter I discusses the application of traditional State and Federal statutes to computer related crime prosecutions. For both levels of jurisdiction, general categories of criminal statutes are presented and discussed in terms of their usefulness in certain types of cases, and also in terms of their general weaknesses as bases for criminal prosecutions. The chapter is supplemented by two appendices which provide citations and descriptions of a sample of existing State and Federal statutes possibly relevant to computer related crime prosecutions.

Chapter II focuses on a wide range of procedural issues associated with the prosecution of computer related crimes, including the admissibility of evidence. Two appendices supplement the chapter. One presents citations and brief abstracts on selected computer related crime evidence cases. The other lists the States which regard computer generated evidence as hearsay, and cites governing provisions.

Chapter III affords specific attention to the issue of privacy and security as it arises in connection with the issues of computer computer related crime. This chapter attempts to outline a number of Federal statutes concerning privacy and security which may be relevant to computer related crime prosecutions. In addition, this chapter provides an overview of the availability of State statutes relating to privacy and security which may prove useful to prosecutors. The chapter is supplemented by an appendix which provides citations and descriptions of a sample of State statutes concerned with privacy and security which are of possible relevance to computer related crime prosecutions.

Chapter IV provides a brief overview of existing and proposed State and Federal computer related crime legislation. Two appendices are provided. One lists and cites recently proposed or enacted State level legislation. The other provides a brief abstract on the proposed Federal Computer Systems Protection Act.

In addition to the Legislative Resource Manual, criminal justice practitioners involved in the investigation and prosecution of computer related crime cases may wish to refer to two other documents published by the Bureau of Justice Statistics. Computer Crime: Criminal Justice Resource Manual is designed to provide criminal justice personnel with a basic understanding of the subject of computer related crime. Computer Crime: Expert Witness Manual provides specific technical guidance to investigators and prosecutors contemplating the use of outside experts as behind the scenes advisers and/or as expert witnesses in computer related crime cases. Both documents are available through the U.S. Government Printing Office, Washington, D.C. 20402.

The reader is advised that the Manual is not intended to serve as an inclusive review of the legislation and caselaw relating to computer related crime. Further, it is possible that modifications may well have occurred in the body or interpretation of law at both the State and Federal levels subsequent to publication of this document. Rather, the Manual is intended to serve as background to the practitioner involved in computer related crime cases.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

CHAPTER I: TRADITIONAL CRIMINAL LAWS

Traditional criminal statutes in most States have been modified through the years to reflect the theories of modern criminal justice, as reflected by U.S. Supreme Court decisions and the economics of administering our system of criminal justice. However, these laws generally envision application to situations involving traditional types of criminal activity. Unfortunately, the modern criminal has kept apace with advances in technology; he has found ways to apply such innovations as the computer to his criminal ventures. Unknowingly, and probably unintentionally, he has also revealed the difficulties in applying older, traditional laws to situations involving non-traditional crimes. For our purposes, such "non-traditional" crimes are crimes against computers or computer assisted crimes.

The subject of applying traditional criminal laws to computer related crimes is particularly complex because, while the computer itself ("hardware") can usually be discussed in terms of traditional forms of property, the intangible but still valuable computer information ("software") will usually not fit this mold. This chapter will look at the application of traditional laws to situations involving both hardware and software.

TRADITIONAL CRIMINAL LAWS AT THE STATE LEVEL

This section will describe the possible applicability of 10 primary types of traditional State statutes to computer related crime cases. Statutory provisions in particular States will be cited. Significant variations in parallel State statutes will also be noted.

Arson

Under the common law, arson is defined as the malicious burning of the dwelling house of another. Modern statutes have dropped the "dwelling house" requirement, and categorized the offense as first, second or third degree arson, depending on the building involved and the purpose of the burning.

In relation to computers, it is clear that the computer itself may be damaged as a result of an electrical fire set intentionally. In addition, stored computer tapes or programs may be burned for unlawful purposes, such as covering up the evidence of a crime or industrial or military sabotage. The use of the arson statute, alone or in conjunction with other State statutes, could prove very effective in prosecuting attacks on computers where it can be proven that damage occurred as the result of a malicious burning.

Criminal ("Malicious") Mischief

Willful destruction of the property of another constitutes "criminal mischief," sometimes termed "malicious mischief". This offense, as with arson, requires an actual human action, observable to a bystander, and tangible damage to property. In computer related crime situations, a distinction must be made between damage to computer hardware and damage to software. Hardware damage can be measured and appraised in traditional ways, but software, though tampered with, may appear undamaged or actually be unchanged. For example, a programmer could conceivably program a computer to override or erase the program's error detection keys, thus employing the computer as an agent in the crime. The damage could be delayed until the proper sequence of keys caused the computer to "remember" its instructions to override or erase.

There are six jurisdictions which define criminal mischief in terms of the malicious injury or destruction of personal property of another. These States are California, Delaware, the District of Columbia, Florida, Massachusetts and Virginia. Most of these States provide for classes of the offense, depending, once again, on the value of the damage done to the property. For example, New Jersey expands this law to allow that if an accused can prove that the amount of damages is less than $200, the charge must be reduced to disorderly conduct.[1] The Illinois Criminal Mischief Statute is the most flexible of all for our purposes because it specifically proscribes damage to "articles representing trade secrets" and because it defines property as "anything of value", including articles representing secret scientific material.[2] Though such a criminal mischief statute may have applicability in prosecuting attacks against computer hardware, problems exist in using such a law to prosecute malicious attacks against software if electronic impulses and software programs have not been accepted as "writing" or "property".

Burglary

Under the laws of most States, the offense of burglary involves the unauthorized breaking and entering of the property of another with intent to commit a crime. Many States, for example New York, Pennsylvania and Delaware, recognize as a defense to this charge the claim of a "privileged entry".[3] Other States, for example New Jersey and Illinois, do not recognize this claim as a defense to a charge of burglary.[4] Massachusetts maintains two laws which may be used against the burglar: the State Burglary Statute, which generally requires a "breaking", and the "Stealing in a Building" Statute.[5] Since the Stealing-in-a-Building Statute creates a separate offense, it has been argued that a suspect could be charged under the State's Larceny Statute as well as the Burglary Statute.[6] Other States, including Texas, recognize the defense of "effective consent",

where the accused in fact received some form of consent to enter the premises.[7] At issue in such a defense would be the extent of the consent and the kind of premises involved.

Where an individual enters a computer facility in an unlawful manner, or for an unlawful purpose, a burglary statute could be applied in the traditional manner. If the accused has entered the facility to damage the computer hardware, steal the software or steal computer time, the mere entering with unlawful intent will be sufficient to prosecute the case. However, where an individual attempts to gain access to the computer's software data in order to steal valuable information (e.g., customer lists, trade secrets, and the like) stored in the computer, prosecuting under a traditional burglary statute could well be futile. Access to the computer could be gained via remote terminals located at one's own home, or via secret telephone codes. Such non-traditional forms of "breaking" and "entering" would not be covered by such a law.

Larceny

At common law, larceny was defined as the felonious taking and carrying away of the personal property of another without his consent, and with the intention of permanently depriving him of it. Where the taking involves computer hardware such as minicomputers, magnetic tape or discs or computer programs, such a traditional theft-of-property concept does not present difficulties for prosecution. However, where the taking involves intangible software, it becomes much more difficult to prosecute under a traditional larceny statute.

Computer software may be "taken" by means of a "patch" from a remote computer terminal; such a "taking" does not affect the hardware and may not even affect the software, since the encoded information may be only recorded (i.e., "copied") elsewhere without ever leaving the main computer. In addition, the "taking" may be done by obliterating the computer tape or program, thereby leaving no trace for prosecutors to follow.

Traditional theft statutes refer to "property", but not all jurisdictions recognize computer software as property. Though New York's larceny statute defines property as "money, personal property...or any article, substance or thing of value", that State's courts recognize as "property" any tangible or intangible item that is capable of being owned or transferred.[8] In Texas, State courts have also interpreted computer software as property.[9] Similarly, a California court upheld a theft conviction where the property was a paper containing customer lists.[10] New Jersey's Larceny Statute covers tangible property, certain listed intangibles, and anything else capable of ownership.[11] The courts have begun to recognize the importance of and difficulties inherent in computer related crime cases, which typify

the incongruence of modern business practices and our traditional criminal laws. However, progress, because it must be made State-by-State, has been erratic.

Theft (or Misappropriation) of Trade Secrets

This offense has been defined as the unlawful taking of "secret scientific material".[12] The crime of stealing trade secrets may exist separately from the general larceny statute in some States, may be subsumed into that statute in other States, or may be imputed into the larceny statute as "property" or a "thing of value". Theft of trade secrets can arise from both the physical stealing and from the copying of the article constituting the trade secret.

The common law requirement for theft that there be a taking "away" fails to address modern methods of copying or stealing trade secrets which do not alter the original nor physically remove it from the owner's possession. Under the Illinois Larceny Statute, for example, trade secrets are regarded as "property", but the Statute also defines theft as obtaining or exerting "unauthorized control" over the property of another.[13] This could be interpreted as an elimination of the transportation, or "taking away", requirement. Texas has a statute governing theft of trade secrets which is separate from its general Larceny Statute and which proscribes "stealing, copying, communicating or transmitting a trade secret without the effective consent" of the owner of the secret.[14]

In four jurisdictions, trade secrets are virtually unprotected. Though Delaware, Virginia, the District of Columbia and Florida all have general larceny statutes, none has a separate theft-of-trade secrets statute, and none has attempted to cover theft-of-trade secrets under its larceny statute. Because these jurisdictions retain the transportation requirement, it would appear that one could not be charged under their larceny statutes for unlawful access, or copying, or memorizing the trade secret of another. An additional problem arises when one considers the larceny requirement that it be shown that the accused intended to deprive the owner of his property permanently. Computer crime felons may have no intention of depriving their victims of "property" at all.

Theft of trade secrets in many States may be prosecuted under the general larceny statute, or in others under a specific statute aimed at trade secrets, but the sophisticated criminal will be careful not to leave traces for prosecutors to follow. Valuable information may be taken or copied without leaving a trace that the computer was penetrated, or that the software has been compromised. Even where there exists an effective theft statute, the felon may still "fall through the cracks" because of prosecutorial inexperience at handling high technology crimes, inadequate funding, complex entry and output records, and/or the inability of the State to establish a prima facie case that there was in fact a "theft" or "taking away" of "property" within the meaning of existing State law.

Embezzlement

The unlawful appropriation of the property of another by one who has lawful possession of the property constitutes the crime of embezzlement. Under California law, embezzlement is defined as the "fraudulent" appropriation of another's property by a person in a position of trust.[15] Most statutory constructions in other States follow this type of language. Although the embezzler has lawful possession, he must still "appropriate" property in a fraudulent manner, and convert it to his own use. The property being converted may be computer hardware, but it is more likely that the felon will appropriate software, such as computer tapes, programs, printouts, and the like. Although the hardware may be expensive, it is not unique. However, the software may be the only compilation of its kind in existence, thereby being invaluable.

Under embezzlement statutes, property may take several forms, including securities, stocks and loans. Because of the large number of financial accounts that may be handled by one computer, and, in turn, by one computer programmer, embezzlement presents the computer criminal with access to an almost unlimited amount of funds plus a means to perpetrate the crime, as well as the possible means to cover his tracks. For example, a computer programmer for a California savings and loan institution transferred money from 41 different accounts into his spouse's savings account by using the institution's computer. He was convicted of embezzlement.[16]

Embezzlement statutes were designed originally to be used in a business environment that kept paper records. Although computer stored data comes from and can be returned to paper records, the information is primarily used in its electronic form. It is this particular characteristic of computerized information that permits the embezzler to carry out his crime with a significant chance to avoid detection.

Receipt of Stolen Property

This offense requires that the stolen property actually be received; that the one who receives it must know (or reasonably suspect) that the property was stolen; and that the actual receiving be done with the intent to deprive the owner permanently of his property. Although some States have created a separate statute to cover this offense, others have attempted to

incorporate the crime into their general larceny statute. Massachusetts has gone a step further; its law provides that one who knowingly receives stolen trade secrets is punishable almost to the same extent as one who steals trade secrets.[17]

In most computer related crime cases, the property involved will have some value to the owner and will therefore be of value to another party. Excluding situations where computer tapes are held for ransom, receipt of stolen property statutes will have general applicability to computer related crime situations. In addition, the use of a computer to obtain information or goods and services, or even high credit ratings, can be prosecuted under most receipt-of-stolen-property statutes. (However, there may be some difficulty in tracing the property in complex cases.) This type of statute is a direct offshoot of the law of larceny, and the prosecution can be expected to face essentially the same hurdles in defining computer software as "property" within the meaning of the law as they do when proceeding under a larceny statute.

Theft of Services or Labor Under False Pretenses

This offense requires that there be a representation made to the victim by the perpetrator; that such representation be made with the knowledge that the representation (of a past or present material fact) is false; and that it be made with the intention of obtaining the property of another. In addition, there must be an actual reliance by the victim on the false representation, and some resultant injury to him.

This offense is actually a form of larceny and, as such, it has been proscribed by statute in many States. A number of jurisdictions have also passed theft-of-credit-card statutes, to cover credit card fraud schemes such as acquiring another's personal credit card or credit account number for unlawful purposes. Whether the crime comes under the general theft-of-services statute or the more specific "credit card" statute, such laws are designed to protect against "false pretenses" theft. Because of the widespread use of credit cards today, this latter type of statute may actually be applied more frequently than a traditional theft-of-services statute.

Under Delaware law, "credit card" includes writings, numbers or other evidences or undertakings to pay for property within the meaning of the statute.[18] However, in Virginia, the scope of the statute is defined narrowly--"instrument or device" used to pay for property.[19] The narrowness of a definition such as Virginia's can be a serious obstacle to prosecuting an individual under a theft-of-services-or-labor-under-false-pretenses statute. For example, a department store may provide credit for established customers, and have credit records stored on computer. However, no credit cards are actually issued. One individual could make a

false representation to sales personnel based on another customer's credit line. The criminal could then obtain property, but with regard to the statute, he could fall between the cracks. That is, he or she could succeed in the perpetration of the crime and, even though a false representation was made, where the statutory language requires the felon to use some "instrument or device" this element would be missing. The intangibility of "credit" may create difficulties for the prosecution; other statutes might, however, be employed tangentially and effectively in such situations.

In New York, the theft of services law covers goods and services and other tangible things of value, but it is unclear whether intangibles would be covered, as well. Where an individual is able to obtain an intangible, such as another's credit card or card number, and in turn use this intangible property to obtain other--tangible--property, both under false pretenses, the prosecution may be hard pressed to make its case at either level. Many statutes have yet to consider the problem of using intangible methods as a means of obtaining tangible property under false pretenses. However, some States have passed statutes which cover false telephonic communications with intent to defraud. These statutes could be employed in situations where a felon uses the telephone to obtain credit card information from computer software to be relayed to a remote terminal. Case law, though, is undeveloped and some States, such as California, require that the message being relayed must be false.[20] Such a requirement would seriously limit the use of this statute in computer software cases.

Interference With Use Statutes

Unauthorized interference with or tampering with, or unauthorized use of another's property which results in a loss to the property owner, is often proscribed specifically by statute. Sometimes referred to as "anti-tampering" statutes, these laws cover a form of computer related crime that may encompass elements of malicious mischief, theft-of-services or theft-of-labor, and forgery. For example, New York's anti-tampering statutes proscribe an array of activities, including tampering with a publicly-owned computer operation, tampering with any property which causes substantial inconvenience, and creating a risk of substantial damage to property, whether or not the damage actually occurs.[21] California and Virginia both base their interference-with-use statutes on a criminal trespass theory, but the Virginia statute reaches any interference affecting the rights of the "owner, user or occupant" of the structure in question.[22]

Since computer facilities require some form of housing both for hardware and software, these trespass-based interference statutes provide the same essential coverage as ordinary trespass statutes. However, the prosecutor has the option of charging the accused under the tampering aspect of the law. Application of

interference-with-use statutes may be an effective means to prosecute the computer criminal whose conduct is not clearly characterized as physical trespass, such as obliterations or bugging of computer software.

Forgery

Forgery is defined as the false making or material altering, with intent to defraud, of any writing which, if genuine, would be of legal efficacy or the foundation of legal liability. Although many jurisdictions have retained common law requirements of the crime of forgery (i.e., signature and document), many others have modified the offense by statute to include the making, altering, execution or authentication of any seal, signature, writing, emblem, or symbol of privilege or identification, with intent to defraud or injure another.

In the area of computer related crime, an individual needs initially to obtain access to computer software, or to utilization of computer time to come within the purview of this law. To avoid detection and prosecution, he would necessarily utilize the entry identification code of another, either directly to injure the other's account or to use the entry code as a means to get computer time or information.

In New York, the forgery statute refers to a "written instrument" which has been altered or made for the disadvantage or advantage of a third party.[23] However, this term is defined to include symbols or identification. It also appears that under this definition of written instrument, a computer felon who used an account number or printed entry code would be subject to the statute. California proscribes the counterfeiting or forging of the "seal or hand-writing" of another, but there remains some question as to whether computer entry codes would fall within this language.[24]

A number of jurisdictions have adopted aspects of the American Law Institute's Model Penal Code's section on forgery (§244.1), which covers any false making of "private writings" which might operate to the prejudice of another. These jurisdictions include Delaware, Texas, the District of Columbia and Pennsylvania. Although computer entry codes must be obtained and used with intent to defraud, where the statutory language is narrowly drawn it may become necessary to show that the entry codes are transferable into written or printed form, for purposes of prosecuting the offense as forgery.

TRADITIONAL CRIMINAL LAWS AT THE FEDERAL LEVEL

In addition to the traditional State laws described in the preceding section, there exists a group of traditional Federal

statutes that could be applied successfully to particular types of computer related crime. These are described in this section. Several of these parallel State statutes which proscribe certain kinds of conduct; these make the same acts illegal when committed within the Federal jurisdiction. Others proscribe conduct which falls uniquely within the Federal domain.

Arson

Federal law defines arson as willfully and maliciously setting fire to or burning "any building, structure or vessel, any machinery or building materials or supplies, military or naval stores, munitions of war, or any structural aids or appliances for navigation or shipping." This statute proscribes arson within special maritime and territorial jurisdictions, but fails to specify whether the language of "any machinery..military or naval stores..or any structural aids or appliances" would encompass computer hardware or software. Although the hardware would probably come under the "machinery" term, software arguably would not. In addition, the computer hardware/software must be used for a listed purpose and the facility damaged must be enclosed within the special Federal jurisdiction.

Where a foreign operative or member of organized crime gains access to a Government computer storage facility and proceeds to burn computer tapes, there may be some difficulty in characterizing the tapes as "machinery", "military or naval stores", or " "structural aids or appliances". If the information stored on the tapes is clearly non-military and non-naval (such as confidential lists of Federal undercover drug enforcement agents), the prosecutor's case is that much weakened by the apparent inability to bring the burned tapes under the statute. Except for limited use with special computer hardware within a special Federal jurisdiction, this statute appears to be too limited to be of much assistance to the prosecutor.

Conspiracy

Federal law (18 USC §371) prohibits a combination or agreement between two or more persons to commit an unlawful act, or to commit a lawful act in an unlawful manner. Under Federal law, it is unlawful for two or more persons to "conspire either to commit any offense" against the United States, or to conspire to defraud the U.S. or any Federal agency "in any manner or for any purpose", so long as one or more persons does "any act to effect the object of the conspiracy." Although, traditionally, broad language in a statute has not withstood close judicial scrutiny, this Act has been upheld because of the danger posed to the country by the absence of such an all-encompassing law. The U.S. Supreme Court has ruled that the statute is constitutional

and that the language is broad enough to include "any conspiracy for the purpose of impairing, obstructing, or defeating the lawful functions of any Department of Government".[25]

Because most banks and many other credit institutions are members of the Federal Deposit Insurance Corporation (FDIC), any actions against such banks and institutions can be imputed to that branch of the Federal Government. Although the statute requires that at least two persons be involved, this statute could have great utility in cases where a conspiracy existed for the purpose of defrauding the Government.

Forgery

Under Federal law, (18 USC §472) it is unlawful to pass, utter, publish, or sell, or attempt the same, or to bring into the U.S., or keep in one's possession or conceal "any falsely made, forged, counterfeited, or altered obligation or other security of the United States" with intent to defraud. Also regulated (18 USC §473) are the actions of one who "buys, sells, exchanges, transfers, receives or delivers" similarly forged or altered obligations or securities.

These laws provide the prosecution with a means of attacking those who use computers to deal in counterfeit obligations or securities. Although sections were amended to exclude notes of banking associations from the definition of "obligation", the statutory language is sufficiently broad so as to arguably allow some forms of computer software within this list of regulated documents.

These forgery statutes could be effective in prosecutions where counterfeit securities are involved and the uttering and/or dealing in them is provable. But where the securities are moved via an electronic funds transfer system (EFTS) and no forgery, counterfeiting or alteration occurs, this form of uttering could be challenged by the defense as outside the parameters of the statutory language. Traditional means of uttering and dealing can be dealt with under the forgery statutes, but computer technology has opened new methods of accomplishing these purposes; these are untried areas for prosecution.

Fraudulent Use of Credit Cards Statute

Federal law (15 USC §1644) proscribes a wide range of credit card abuses, including the use, attempt or conspiracy to use "any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card to obtain money, goods, services, or anything else of value"; "transporting or attempting or conspiring to transport a fraudulent or unlawfully obtained

card"; "using with fraudulent intent" such a card; "knowing receipt, concealment, use or transport of goods, services, or tickets for interstate or foreign transportation" obtained by use of such card; and the "furnishings of money through use" of such an unlawfully obtained card.

Although the Statute employs a broad proscription against fraudulently obtaining "anything else of value", there is an absence of clear language as to what constitutes "use". This becomes most important where the mere uttering over a telephone of an individual's credit card number is the means by which a fraud is perpetrated. In addition, in such a situation the actual obtaining of the credit card itself never occurred, so the langauge fails to address situations where only the account number is misused. Where the felon fails to meet the specified dollar amounts proscribed by the act or fails to affect or engage in interstate or foreign commerce, this Federal statute will have no applicability.

Embezzlement and Theft Statute

Federal Law (18 USC §641) proscribes embezzling, stealing, purloining, or knowing conversion, or the receipt, concealment, or retaining or "any record, voucher, money, or thing of value" of the Federal Government with intent to convert it to one's own use or gain. This is another statute whose references to public money, property or records may be interpreted broadly enough to include new forms of computer related offenses which could fall within the statutory language.

This Statute covers one who receives, conceals or retains Federal property for his own use--a type of receipt-of-stolen-property statute. However, the definition of "records" has not been specifically modified to include computer printouts, programs, and the like.

Theft of Goods Moving in Interstate or Foreign Commerce

A Federal statute (18 USC §659) makes it unlawful for anyone to embezzle, steal, or unlawfully take, carry away or conceal, or fraudulently obtain "any goods or chattels moving as or which are a part of" interstate or foreign commerce. The Act also encompasses the buying, receiving, or possessing knowingly of such property, and its reach extends to any successive jurisdictions within the U.S. in which the felon may have taken or been in possession of the goods.

However, this law was framed with traditional, tangible goods in mind. The transfer of encoded information from one computer terminal to another across State lines may not necessarily

come under this Statute. There may be difficulty in characterizing computer services or information as "goods or chattels". In addition, frequently there are no bills of lading or shipping documents in computer related transactions. The law makes no reference to computer services. It is unsettled whether computer "time" and functions would constitute "goods or chattels" under the Statute.

Interstate Transportation of Stolen Property

Federal law (18 USC §2314) proscribes interstate transportation of stolen property and it specifies those items which are to be considered "property", such as "goods, wares, merchandise, securities or money..tax stamps..traveler's check(s)..and any tool, implement, or thing used or fitted to be used in falsely making, forging, altering, or counterfeiting" any of the listed items. However, this Statute is limited in that it does not apply to any falsely made, forged or altered obligation, bond or promissory note issued by "any foreign government or by a bank or corporation of any foreign country." This limitation can be fatal to a prosecution that involves domestic criminal activity yet also a forged foreign document. In addition, the law faces many of the same problems as other statutes which have not defined computer software, data and services as "property".

Mail Fraud and Wire Fraud Statutes

Federal laws (18 USC §§1341, 1342) proscribe the use of the mails and wire services to perpetrate a fraud. The mail fraud statute refers only to the U.S. Postal Service; it leaves unprotected such private carriers as United Parcel Service and Federal Express, to name only two. This Mail Fraud Statute does proscribe the use of fictitious names or addresses to perpetrate or further a fraudulent scheme, however. The Wire Fraud Statute regulates wire, radio or television communications in interstate commerce with regard to any fraudulent scheme.

In 1976, a former employee of a national computer firm was charged with wire fraud.[26] In his former employment the defendant had obtained access to secret computer key codes. He retained this knowledge when he left the computer firm. Subsequently, he used a telephone and a remote computer terminal to dial the computer's telephone number and penetrated a fraud on the computer. Over a period of several months, the defendant repeatedly gained access to the computer's secret codes, and obtained information that was passed over the wires from the victim firm's offices in Maryland to the defendant's office in Virginia. Though the distance was not great, it did cross State lines.

The defendant's objective in repeated calls to the computer was to extract a computer program developed for the firm. Before he was detected, the defendant had managed to extract 18 of the 20 codes necessary to gain information stored within the computer. The program was the valuable object in pursuit, not the information of any of the Federal agencies which utilized the firm's computer services.

In finding the defendant guilty, the Federal court determined that the computer program was a trade secret, a form of "property" with proprietary rights. The court based its finding of guilty primarily on the fact that the fraud in this case was perpetrated by use of the wires and involved a communication which crossed interstate lines. Although the Wire Fraud Statute was used effectively in this case, it was fortunate for the prosecution that the defendant made his phone calls to the firm's computer from his Virginia office, rather than his Maryland home; a call from his residence to the computer firm--both located in the same State--would have precluded the application of the Federal Wire Fraud Statute completely.

Interception of Wire or Oral Communications

Under Federal law (18 USC §2511) it is unlawful to willfully intercept, attempt to intercept, or procure another person to intercept, or willfully use or procure another to use "any electronic, mechanical, or other device" to intercept any wire or oral communication. In addition, it is unlawful to manufacture, distribute, possess or advertise any device used for intercepting wire or oral communications, and the disclosure or use of the contents of "any wire or oral communication, knowing or having reason to know that the information was obtained unlawfully". This law, referred to as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, was designed to protect the privacy of wire and oral communications of common carriers, not to protect financial institutions. Wire communication is defined in the Act as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection...furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications". Where the computer data is not furnished or operated by a person engaged as a common carrier or where the communication does not cross State lines, the law will not apply.

Oral communication is defined as any oral communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation". However, the law will not apply to situations involving interception of encoded information that is "audible" only as blips and bleeps, but not "uttered". Further,

the utterer must not only have an expectation of privacy, but must also "exhibit" this expectation, under appropriate circumstances. Moreover, the law is designed to protect only the "privacy of innocent persons".[27]

Under this Act, "intercept" means any "aural acquisition of the contents of any wire or oral communication". This requirement might be impossible to meet in computer related crime situations where encoded computer information may be aurally acquired, but completely unintelligible. With regard to oral communication, it is clear that a person will never utter computer data. The "machine language" of computers is not a language in the sense that it can be physically learned and mastered by humans; they will always need a computer to translate machine language to human language.

CONCLUSIONS

Although there are a plethora of statutes which may be used against traditional criminal offenses, and although many of these same statutes may be applied to computer related crimes with some degree of success, it is clear that many cases may fail to reach prosecution or result in convictions because of the gaps which currently exist in the Federal Criminal Code and in the arsenal of State criminal statutes. Most State and Federal criminal statutes were designed to combat familiar, cognizable, and measurable offenses, which generally left behind an injured victim and a trail to follow. Computer related crime defies this description of the traditional criminal offense. It makes prosecution, even by the well-initiated, an extremely difficult undertaking under most existing statutes.

It should be recognized that the statutory provisions described above are subject to varying interpretations, and that more expansive interpretations which encompass computer crime may exist or evolve over time. Additionally, such statutes may of course be modified through legislative action or judicial ruling.

FOOTNOTES--TRADITIONAL CRIMINAL LAWS

1. State v. Tonnisen, 92 N.J. Super. 452, 224 A.2d 21 (1966).
2. 38 Ill. Ann. Stat., sec. 21-1; sec. 15-1.
3. N.Y. Penal Law, sec. 140.00(5); 18 Pa. Stat. Ann., secs. 3502, 3930(a); 11 Dela. Code Ann., sec. 829(d).
4. N.J. Stat. Ann., sec. 2A:94-1 (1969); State v. Martinez, 112 N.J. Super. 552, 272 A.2d 289 (1970); 38 Ill. Ann. Stat., sec. 19-1 (Supp. 1975).
5. 266 Mass. Gen. Laws, secs. 16, 16A, 17 and 18; 266 Mass. Gen. Laws, sec. 20.
6. Susan H. Nycum, "Legal Sanctions to Computer Abuse," Assets Protection, Vol. 2, No. 3, 1977, p.33.
7. Tex. Stat. Ann., Penal Code, sec. 30.02(a).
8. N.Y. Penal Law, sec. 155.00(1).
9. Nycum, "Legal Sanctions to Computer Abuse", (see note 6, supra).
10. Ibid.
11. N.J. Stat. Ann., sec. 1:1-2; see also sec. 2A:119-5.3.
12. N.Y. Penal Law, sec. 155.30(4).
13. 38 Ill. Ann Stat., sec. 15-1.
14. Tex. Stat. Ann., Penal Code, sec. 31.05.
15. Cal. Penal Code, sec. 499c(b)(2).
16. Computer Crime--Criminal Justice Resource Manual (LEAA) (Washington, D.C.: U.S. Government Printing Office 1980), p. 354, Case No. 7333.
17. 266 Mass. Gen. Laws, sec. 60A.
18. 11 Dela. Code Ann., sec. 904.
19. Va. Code Ann., sec. 18.1-125.2(2).
20. People v. Rand, 23 Cal. App. 3d 579, 100 Cal. Rptr. 473 (1972).
21. N.Y. Penal Law, secs. 145.15, 145.20, 145.25.
22. Va. Code Ann., sec. 18.1-183 (Supp. 1974).

23. N.Y. Penal Law, sec. 170.00(1), et seq.

24. Cal. Penal Code, sec. 470.

25. Haas v. Henkel. 216 U.S. 462, 30 S.Ct. 249 (1909).

26. U.S. v. Bertram E. Seidlitz, 589 F.2d 152 (1978).

27. 18 U.S.C., sec. 2511, Congressional Findings, sec. d.

CHAPTER II: EVIDENTIARY AND OTHER PROCEDURAL ISSUES

Constitutional and statutory procedural safeguards are designed to provide the defendant with an adequate opportunity to challenge his accuser and to challenge the evidence proffered against him. Many of these procedural safeguards have their roots in the English common law. Prosecutors handling computer related criminal cases must, therefore, work within this evidentiary and procedural framework. Those prosecutors who seek to have computer generated records admitted into evidence must first overcome several serious procedural challenges before a court will admit the records. A presentation of the primary procedural issues the prosecution will face follows in this chapter.

The material presented below is supplemented by that which appears in Appendices "C" and "D" to this volume. Appendix "C" presents citations and brief abstracts on selected computer related crime evidence cases, while Appendix "D" notes which States regard computer generated evidence as hearsay, and provides citations to the governing provisions within their respective codes.

OBTAINING EVIDENCE

Computer crime may well be the subject of both civil and criminal litigation in either Federal or State forums. With regard to civil litigation, both judicial proceedings and various administrative law proceedings are possible options. In all such proceedings, a common concern of the adjudicatory authority must be to obtain jurisdiction over persons and records relevant to the case and to secure the presence of such persons and documents before the tribunal. This section addresses key issues involved in the successful production of computer generated records for adjudicatory proceedings.

Administrative Searches

Many Federal Government agencies such as the Federal Trade Commission and the Securities and Exchange Commission may conduct investigations through the use of administrative subpoenas, and can refer appropriate cases to the Justice Department for criminal prosecution. Traditionally, the courts have allowed these agencies to conduct regulatory or administrative searches on the ground that such searches are essentially civil in nature.

In the prosecution of computer related offenses, the defense may move to suppress evidence obtained as a result of administra-

tive searches (Rule 16, Fed. Rules Crim. Proc.), but the burden is then on the defendant to prove that the intent of the search was to develop a criminal case. This area of law is unsettled and court decisions are inconsistent concerning the use in criminal proceedings of material discovered by non-criminally restricted agency or administrative searches.

Subpoena Duces Tecum

In securing the physical possession of relevant computer records and printouts, the prosecution must move carefully, but quickly. Because of the speed and facility with which computer information can be destroyed, a subpoena duces tecum may be one of the most effective means of securing tapes or other software by requiring the defendant to produce them before a grand jury (Fed. Rule Crim. Proc. 17[c]). However, the subpoena also gives the felon specific notice as to what is being sought (and hence what he should destroy). The subpoena is also subject to a motion to quash.

Search Warrants

Use of a search warrant can be very effective in securing relevant computer related information, but the warrant must be sufficiently broad to encompass the possibly large number of records needed to make the case, and not too broad so as to be struck down as a mere "fishing expedition". However, the warrant will not issue without a showing of probable cause that the information sought will support the alleged offense. In addition, the Fourth Amendment requires that a search warrant provide a specific description of the items to be seized, and the corporation whose records are involved is a "person" under the law, thereby entitled to full constitutional protection.

Consent Search

A consent search is preferable to obtaining a search warrant, but a valid consent must be secured from one who has custody of the records and who has authority to give consent. In addition, the consent must be knowing and voluntary, that is, the party must be informed of the scope and purpose of the search, and the party must not be under any duress or coercion, or threat of coercion, to give consent. Failure to demonstrate that the consent was valid could be fatal to the prosecution. Because a search warrant can be suppressed, and because a request for a consent search could lead to destruction of the evidence sought, it has been suggested that the prosecution initially obtain the warrant, request a consent search, and then use the warrant if

the consent is denied.[1] This would provide the prosecution with a double-barrelled approach to the evidence, and it avoids exposing the evidence to destruction.

Exigent Circumstances

The doctrine of exigent circumstances has been recognized by courts as applicable to a variety of situations where, if law enforcement were to delay so as to obtain a search warrant, the suspect(s) would flee and/or irreplacable evidence would be destroyed. The "hot pursuit" of a fleeing felon across jurisdictional lines or into a dwelling is one example of the application of this doctrine; "no knock" drug raids is another. Given the ease with which data stored in computer software or hardware can be altered or destroyed, the doctrine of exigent circumstances might successfully be applied to a warrentless search and seizure of computer related evidence. Successful investigations in at least one State, which ended in negotiated pleas of guilty, suggest that this doctrine is of possible applicability in computer related crime cases, under at least certain circumstances.

INTERROGATIONS AND AFFADAVITS

Custodial interrogations of suspected computer felons must meet the requirements of the Miranda decision. The suspect must be informed of the following:

- that he has the right to remain silent,
- that anything he says may be used against him,
- that he has the right to counsel, and
- that if he is financially unable to retain counsel the the court will appoint counsel to represent him.[2]

As with consent searches, a waiver of these rights must clearly be voluntary.

The majority of computer crime cases will involve professionals whose education and background have enabled them to secure trusted positions within their respective companies' computer divisions. The typical suspect may not need the services of court appointed counsel, and may possibly even be an attorney. Nevertheless, prosecutors should not overlook the importance of informing each and every suspect involved in custodial interrogations of his or her rights. A voluntary confession is invaluable to the prosecution, but an uninformed confession is virtually worthless.

As has been noted, many computer related crime suspects are highly educated and sophisticated and may have effective assistance of counsel easily at hand. Voluntary confessions and successful custodial interrogations are comparatively unlikely occurrences in such cases. A useful investigatory technique may be to request sworn affadavits from suspects, which will require them to state under oath that they did not engage in the illegal actions suspected. An unwillingness to provide such an affadavit may warrant increased investigatory activity. In the event that an affadavit is provided and the suspect is later successfully prosecuted, a perjury conviction can then also be sought.

ADMISSION OF EVIDENCE

In the area of documentary evidence, two rules have evolved which were deemed necessary for the proper pursuit of justice in a court proceeding--the best evidence and the hearsay rules. Since strict adherence to these rules in all circumstances would be impractical, exceptions evolved.

A key problem with regard to introducing computer records into evidence is the need to establish a proper "foundation" to identify or authenticate the record and to assist in bringing the record within the appropriate exception. A review of reported cases concerning this aspect of computer generated information indicates that there is common difficulty in laying a proper foundation with regard to such evidence. In addition, once the foundation for admissability of computer generated records has been laid, the trustworthiness of the evidence must be demonstrated if it is to withstand defense challenges to its admissability. (See Appendix "C" for a description of leading cases.)

The following sections will address in detail each of these major obstacles to the admissability of computer-generated records--the best evidence rule, the hearsay rule, and procedural problems with regard to laying the foundation. Exceptions to the best evidence and hearsay rules under Federal and State law will be reviewed, and other factors impacting on the successful admission of such evidence will be presented.

THE BEST EVIDENCE RULE

The best evidence rule requires that where a party attempts to prove his case by the use of several types of evidence, he must provide the strongest ("best") evidence available, and not secondary ("copies") evidence. To prove the content of a writing, recording or photograph, the party generally must provide the original writing, recording or photograph.

In cases involving computer stored or computer generated information, the originals may no longer exist, or in fact may never have existed (as in the case of computer analysis or projections). The best evidence rule could easily act as a bar to printouts of such computer data, on the ground that they are "copies" of the originals. Historically, the rule has not barred properly authenticated public documents and has been applied primarily in litigation involving private documents and writings.

In cases where computerized records constitute the only extant account of paper records, courts have consistently held that the computer records are the best evidence available. However, Rule 1001(3) of the new Federal Rules of Evidence now defines as an "original" those data that are stored in a computer or similar device. The best evidence rule does not, therefore, pose a serious obstacle to the introduction in evidence of computer records, tapes or discs in Federal court. The situation with regard to State courts differs considerably from jurisdiction to jurisdiction.

There are two primary exceptions to the best evidence rule--the voluminous writings exception under Federal law and the photographic copies exception under Federal law and the laws of several States.

The Voluminous Writings Exception

The Federal voluminous writings exception provides that where the original writings, recordings, or photographs are so voluminous that it would be impractical to produce them in court, a summary may be allowed in.[3] However, the originals must have been made available to the defendant for examination and copying, at a reasonable time and location. It must also be shown that the material was prepared in summary form by a competent individual. In a now classic case, a State court allowed in evidence a computer printout which was a summary of accounting records, based on the testimony of the company's director of accounting.[4] In a criminal case involving the Franklin National Bank, the prosecution made available to the defense 50 million bank documents in the possession of the Federal Deposit Insurance Corporation. The voluminous writings exception was the most effective means of drawing summaries as exhibits from these records.[5]

The Photographic Copies Exception

An important State level exception to the best evidence rule is the Uniform Photographic Copies of Business and Public Records Act.[6] This model legislation has been adopted by more than 30 States in an attempt to deal with the rule in the context of a

computerized business world. State courts acting under this law may allow in evidence a copy of an original made by "any process". This language is significant in States which do not have specific legislation dealing with the admission of computer generated evidence. A Mississippi court allowed in evidence computer printouts, even though the State had not at that time enacted the Uniform Photographic Copies Act, on the rationale that the information contained on the printouts was a regularly maintained business entry. The court regarded its action as merely accepting a regularly maintained business record, not withstanding "electronic recordkeeping."[7]

The Federal statute which governs photographic copies of records made in the regular course of business has been used in criminal prosecutions involving computer printouts.[8] The statute allows for the admission in evidence of a reproduction that is "satisfactorily identified", and it reaches private as well as government documents. A Federal appeals court ruled that a defendant may inquire into the data processing input and output procedures in his attempt to attack the reliability of a computer printout offered as evidence.[9]

Other Factors Relevant to the Best Evidence Rule

The defendant may challenge computer records as admissible evidence on the basis of the best evidence rule, which, as has been discussed above, provides that no evidence other than the original writing of the event, condition, or act is admissible to prove the content of the writing. Although primarily an evidentiary consideration, this challenge may also involve constitutional protections which require a more in-depth analysis. For example, a Federal appeals court ruled against a gas company that relied solely on its computer in determining which customers would have their service terminated for lack of payment.[10] The customers alleged that their service was terminated in violation of their constitutional right to due process. The computer issued shut-off notices whenever payments were overdue, but there was no system to ascertain the status of the account at the time the notices were issued. Evidence indicated that there was a delay between the time of actual payment and the time the information was fed into the company's computer. The company relied on computer records kept in the regular course of business, but the customers were successful because of their constitutionally-based due process challenge of these records.

Although the company now has a manual system of review before shut-off takes place, and telephone access has been added to the computer facility, this case illustrates the difficulty of adequately determining the accuracy and reliability of the records. In this case, the best evidence was not the computer records, but the customer's written receipt of payment; the time lag can be fatal. However, in a another such case in Georgia, a

time delay of 28 days was found not to preclude admission of the computer records.[11]

Exceptions to the best evidence rule may assist in the admission of computer records as evidence, but the prosecution would be wise to consider all possible constitutional and codified challenges to admission. Cases which have allowed computer records in as evidence to date indicate more a failure on the part of the defendant to raise such challenges than incompetence of the prosecution to lay a proper foundation.

THE HEARSAY RULE

Hearsay evidence is an out-of-court statement, oral or written, offered as truth. Hearsay is a form of evidence that does not proceed from the personal knowledge of the witness, but in reality is merely a repetition of something which the witness heard. Historically, exclusion of this form of evidence was a result of the realization that uncorroborated testimony could be coerced or induced in favor of or against a particular party.

In the prosecution of computer related crimes, the defendant's confrontation right could arguably present problems with regard to computer generated evidence. The defendant facing charges which are to be substantiated by computer records or printouts may inquire into the computer programming procedures and the identities of the programmers, and into the accuracy and reliability of the computer hardware. The computer evidence proffered may be erroneous as a result of inaccurate information being fed into the computer, human error or improper input procedures, accidental or intentional tampering, defective hardware or software, and/or inaccurate or improper output procedures.

The potential for inaccuracy in computer records is considerable. The purpose of the hearsay rule--to preclude the admission of evidence which is unreliable--could easily be applied to bar admission of computer records. As Appendix "D" will illustrate, 38 States currently define computer generated records as hearsay. However, just as exceptions evolved to fit specific circumstances under the best evidence rule, so too have exceptions been recognized to the rule barring hearsay evidence. A primary exception to the hearsay rule as applied to computer related crime cases is the Business Records Exception. The applicability of the exception at the State and Federal levels is discussed below. This is followed by a discussion of other relevant exceptions which may apply in computer related crime cases.

The Business Records Exception

Computer records may avoid the prohibition against admitting hearsay if it can be shown that the records fall within the

"business records" exception to the hearsay rule. This exception provides for the introduction into evidence of records made in the normal course of business which were made contemporaneously with the occurrences that they record, or reasonably shortly thereafter. The record may qualify under this exception by coming in under the new Federal Rules of Evidence or under one of the States, business records laws. Where the governing business records statute does not encompass computerized data, the defendant may argue that computer records do not constitute "records" within the meaning of the Act. Because computer records are not susceptible to human examination in the same way as manually prepared business records, the court may accept the defendant's argument.

Admissibility of Business Records Under the New Federal Rules of Evidence

In 1975, the new Federal Rules of Evidence became law, replacing the mandates of Federal Rule of Civil Procedure 43(a), which directed the Federal courts to State evidence law where no Federal statute or practice provided a more liberal rule, and of Rule 26 of the Federal Rules of Criminal Procedure, which required Federal courts to develop their own criminal evidence rules as Federal common law.[12]

Prior to this time, the Federal Business Records Act of 1936 was the authority under which business records were introduced in evidence, where it was shown that they were books of original entry, made in the usual course of business, and introduced from proper custody and upon authentication.[13] Because of the Rules' stated purpose of "fairness...to the end that truth may be ascertained and proceedings justly determined", the requirements of the Federal Business Records Act have been modified.[14] The new Rules specifically address records kept on regularly conducted business activity.[15] They still provide for the identification and authentication of business records as a condition precedent to admission, but authentication may be satisfied by showing that the computer program or system employed in fact produced the records in question, and the system is known to be accurate.[16] If a company's director of computer operations testifies, for example, that (a) the company's computer system is designed to keep computerized records of all overseas telecommunications, (b) the computer was used for that purpose, and (c) the system used is a software package recognized as accurate when used with this computer for this purpose, then the records may well be admitted.

An important step forward with regard to evidence in the modern business community is the language of the new Rules, which includes within the definition of "writings and recordings", such diverse concepts as "magnetic impulse, mechanical or electronic recording, or other form of data compilation."[17] Although the Rules specifically allow for computer printouts to be deemed

"originals", the requirements that the writing be accurate and authentic are retained. Where prosecutors can demonstrate that the computer system in question is accurate and the process by which the records were programmed into and retrieved from the computer are sound, readable, and not prone to manipulation or fraud, the printout will be allowed as though it were an original document. However, the new Rules still require that records be kept in the regular course of business, that they be entered on or about the time of the event or transaction, and that the records be produced by individuals with knowledge of the information that is recorded.

Under the new Rules (Rule 803(6), at Note 9), a prosecutor may be allowed to enter into evidence "data compilation, in any form". Although most jurisdictions have not yet amended their statutes to encompass computer records within the business records exception, many State courts have followed the lead of Federal courts. Computer records may be allowed into evidence over an objection that they do not constitute "records" within the meaning of the governing statute. (See cases listed in Appendix "C.")

In a related Federal case, a U.S. Court of Appeals upheld the conviction of a man who stole an automobile from a major car rental corporation and drove the vehicle across the United States.[18] Although the defendant had given the police a written confession, his conviction was based on computer records showing that the car had not been rented. The defendant could have challenged the admission of the computer records on several grounds, but the court allowed the records in under the business records exception. The court observed that the Federal statute does not require that the records be in written form.

Admissibility of Business Records Under Various State-Level Exceptions

There are numerous State-level business records exceptions to the hearsay rule. These reflect both the common law and statutory State efforts to formalize the exception. There are essentially five forms or counterparts to the Federal business records exception embodied in the new Federal Rules of Evidence. These are as follows:

- the common law "shop-book" rule;
- the Uniform Rules of Evidence Act;
- the Uniform Business Records as Evidence Act;
- the Texas Act; and
- the ALI Model Code revision.

The Shop-Book Rule

The shop-book rule permits the introduction into evidence of books of original entry made in the usual course of business, introduced by one who has proper custody of the records, and authenticated. The rule today only applies in about a dozen States, and has been modified in a number of other States.[19] The modern requirement of authentication of business records is merely a broad version of the requirements of the shop-book rule, which set four preconditions before records could be admitted in evidence. These are as follows:

- the records must have been made routinely, during the regular course of business;
- the entry must have been made contemporaneously with, or within a reasonable time after the transaction being recorded;
- the entry must have been made by a person who is now unavailable as a witness and who has personal knowledge of the event; and
- the recorder must have had no motive to misrepresent or misstate the facts.

It is a well recognized and accepted practice in transcribing business records into computerized data that a time lag exists which can be a few days or many months. Aside from the computer service's backlog, some companies for policy or economic reasons do not transfer their records until months after an event has occurred. This delay would be fatal to evidence that was proferred under the shop-book rule.

The personal knowledge requirement may defeat the admission of computerized business records because of the practices involved in computer security. Such practices dictate that computer personnel with access to software be rotated to prevent any one individual from having a current means of fraudulently using computer entry codes. In this way, no one person will know more than is necessary for his own job function. Knowledge of a particular record or event under such security practices will become so rare as to be non-existent. Where the computer network is elaborate, is hooked up to other networks or is multinational, the personal knowledge requirement will be all the more difficult to satisfy. Nevertheless, some courts have modified their interpretations of the rule to allow computer printouts in as evidence.

The Uniform Rules of Evidence Act

The Uniform Rules of Evidence Act provides that writings offered as memoranda or records of acts, conditions or events to

prove the facts of those conditions or events may be admitted in evidence if the judge finds that (1) they were made in the regular course of business, at or near the time of the event recorded, and (2) the sources of information from which the records were made and the method and circumstances of their preparation were such as to indicate their trustworthiness.[20] The Act was adopted in 1965 by Kansas, the Virgin Islands, and the Panama Canal Zone (which is no longer under U.S. jurisdiction). The Act was drawn up before the first computer related litigation ever occurred, and clearly did not envision the problems which could arise. The Act conspicuously retained the shop-book rule requirements that records be made in the regular course of business, at or near the time of the event. Although the court is given wider discretion with regard to admitting such evidence, the Act did not gain wide acceptance and is now clearly insufficient to address issues involved in computer related evidence.

The Uniform Business Records as Evidence Act

The Uniform Business Records as Evidence Act provides for the admission into evidence of any writing or record of any act, condition or event "if the custodian or other qualified witness testifies to its identity and to the mode of its preparation, and if it was made in the regular course of business, at or near the time of the act, condition, or event, and if in the opinion of the court, the sources of information, and method and time of preparation were such as to justify its admission."[21]

Since 1936, a total of 26 States have adopted this modified version of the shop-book rule. Significant changes in the rule which are embodied in the language of the Act allow for the possibility that computer records could be considered as a "condition." In addition, a "qualified witness" may substitute for the common law requirement that the record-keeper provide testimony. The Act gives the court discretion to determine whether the circumstances surrounding the recording of the event indicate trustworthiness. This was clearly a step forward from the restrictive language of the shop-book rule.

However, the Act retained two requirements that stand as formidable obstacles to the admission in evidence of computer records--(1) the writing or record must be made in the regular course of business; and (2) the recording must be done at or near the time of the event. In one case, computer printouts were admitted under the Act, despite the fact that the only witness to testify concerning the records encompassed within the printouts was an assistant cashier who stated that the records were prepared by "automatic machine."[22] Another State court admitted computer printouts into evidence over the numerous and substantial objections of the defendent because the purpose of the Act is to permit admission of "systematically entered records without the necessity of identifying, locating and producing as witnesses

the individuals who made entries in the records in the regular course of business.[23] The court ruled that a proper foundation had been laid to admit the printouts in evidence.

These early decisions occurred before professionals and the general public achieved a degree of sophistication concerning computer errors and computer fraud. The courts may have decided to admit computer records in evidence more on the basis of the quantity of the foundation testimony than on the quality of it. Today's litigators are better equipped and more aware of the possible challenges which can be successful with regard to admitting such evidence. The Act, as a revised version of the shop-book rule, has expanded the use of computer records as evidentiary tools in prosecuting computer felons, but it fails to address all the issues necessary to make such evidentiary tools fully effective and available.

The Texas Business Records Act

The Texas Business Records Act allows for the admission into evidence of any relevant memorandum or record of an act, event or condition if the judge finds that (1) it was made in the regular course of business; (2) it was the regular course of that business for an employee or business representative with personal knowledge of the event to make such a record or to transmit that information for inclusion into a memo or record; and (3) it was made at or near the time of the event, or reasonably soon afterward.[24] The Texas Act requires that the employee or business representative who makes the record or transmits information from a memo to the record have personal knowledge of the event within the record. There are no provisions for any other "qualified witness" to testify concerning the records or the record-keeping process, and there are not grants of discretionary authority to judges in cases where the evidence might be accompanied by circumstances indicating trustworthiness.

Texas courts have generally interpreted this statute narrowly and strictly, requiring, for example, that the witness providing the personal knowledge of the information contained in the computer record also possess personal knowledge of the operations of the computer system.[25] Computer punch cards containing data about the company's sales and commission records were ruled inadmissible where the court found that no one who testified had personal knowledge of the information punched on the cards.[26] The Act is clearly a difficult statutory obstacle to the introduction in evidence of computer records, and has gained no support outside of Texas.

The ALI Model Code Revision

The American Law Institute (ALI) Model Code, proposed by that organization, in 1942 contained a provision intended to serve as a revision of the business records exception. Ostensibly, the purpose of the Code provision was to give the courts greater discretion in admitting business records if the records tend "to prove the occurrence of the act or event" and if the judge should find that the records were made "in the regular course of business."[27] The Code requires that the person who made the record have personal knowledge of the information of the event recorded, that the recording be contemporaneous with the event, and that it be made in the regular course of business.

Where a person having personal knowledge transmitted this information to another person who made the actual record of the event, the ALI Model Code authorized that such a record would be admissible if the court was satisfied that the recording met other requirements.[28] The ALI Model Code was an attempt to handle the increasingly complex problems involved in litigation with regard to the needs and requirements of a modern business community, but it was never adopted by any State and otherwise would not have been applicable to deal with the concepts involved in computer records which are proferred as evidence.

OTHER EXCEPTIONS TO THE HEARSAY RULE

In addition to the business records exception, which can be expected to be the one most commonly relied upon when seeking to get computer generated evidence admitted, there are several other traditional exceptions to the hearsay rule of possible applicability to computer related crime cases. These are presented below.

Former testimony exception

Former testimony which was admitted in evidence in an earlier court proceeding will be accepted in the present trial, if it can be shown that (1) the witness whose testimony is being proffered is unavailable for trial; and (2) the defendant has had an opportunity to cross examine the witness. The "unavailability" requirement traditionally has been strictly construed, especially in criminal cases where such evidence, if admitted, could lead to an unjust result. In addition, the unavailability must be permanent in nature, and clearly established. Courts have recognized as unavailable, in addition to persons deceased, persons who were outside the jurisdiction of the court and those physically or mentally incapable of understanding the proceeding. Another form of unavailability is the concept of a "privilege", such as that which has been recognized concerning communications between husband and wife, between attorney and client, and the privileged communications involved in trade secrets and Government secrets.

The reliability of former testimony will undergo severe scrutiny, particularly with regard to computer generated evidence that was admitted in a prior proceeding. The former testimony exception allows the defendant to examine the type and purpose of the manner in which the former testimony was admitted in evidence. Oral testimony as to former testimony and contemporaneous, unofficial notes of one present at the time of the former testimony have been deemed admissible.[29] Where the circumstances surrounding the admission of computer related evidence in a former proceeding indicate permanent unavailability of the witness, past opportunity for cross examination, and reliability of the forum in which the testimony was given, computer records could easily be deemed admissible.

Public Records and Reports; Medical Records Exceptions

Public records and reports and medical records are two additional exceptions to the hearsay rule. The first exception governs records, reports, statements or data compilations "in any form" of the activities of a public officer or agency, matters witnessed pursuant to a statutorily imposed duty (excluding criminal matters observed by law enforcement personnel), and factual findings from an inquiry made pursuant to law, unless the circumstances indicate lack of reliability or trustworthiness.

The medical records exception relates to records or statements made for the purpose of medical diagnosis or treatment, such as information concerning medical history, past or present symptoms, pains and sensations, or possible causes and methods of treatment. Computers have been used to store and retrieve many forms of public and medical records and computer generated reports can be expected to qualify under both of these exceptions.

Where such public records and reports have been computerized, various Federal statutes provide for the admission in evidence of the printouts, tapes, or discs under the basic reasoning of the exception--regularity of recordkeeping and lack of motive to falsify. However, because of the businesslike operations of both a hospital and a physician, most jurisdictions have come to regard medical records and reports in the same light as commercial entries and records. Consequently, the requirements for admissibility are essentially the same as for business records.

The Jencks Act Exception

In criminal proceedings, the Jencks Act exception provides for a defendant's right to demand the production of any statement of a prosecution witness which relates to the subject matter of the witness' testimony.[30] To emphasize the effect and

importance of admitting such evidence, the Act further provides that if the Government elects not to comply with the court's order to produce the statement(s), the court is required to strike from the record the witness' testimony or, in its discretion, declare a mistrial.[31] This provision reflects the legislative intent to protect the defendant's rights to confrontation and due process.

The statute broadly defines "statement" to include a "...mechanical, electrical, or other recording..." which is a substantially verbatim recital of the witness' oral testimony, where the recording occurred at the same time as the utterance.[32] Conceivably, statements which were recorded contemporaneously with the utterance and later computerized could come in under the Jencks Act provisions. With the onset of computerized court transcripts, the exception may receive widespread application in many criminal proceedings. Care should be taken where proffering computer related evidence for admission that the reliability and accuracy of the computer records are established by first establishing a proper foundation.

Recorded Recollection Exception

The recorded recollection exception allows for the admission into evidence of a memorandum or record about a matter of which the witness had knowledge at one time, but now has insufficient recollection to permit him to fully and accurately testify. The memo or record must be shown to have been made or adopted by the witness when the matter was fresh in his memory and to reflect that knowledge accurately.[33] If the record or memorandum is admitted, its contents may be read into evidence, but it may not be admitted as an exhibit unless the defendant so moves.[34]

Where the witness swears that the record was made at the time of the statement, that he read the record and knew it to be true, and the recorder swears to his recording ability and procedures, the court will allow any such recorded recollection into evidence. Once again, it is entirely feasible that computer assisted court transcripts will be admitted, this time under the recorded recollection exception to the hearsay rule.

Present Sense Impression Exception

The exception known as "present sense impression", also known as "present recollection refreshed", provides that a statement describing or explaining an event or condition may be allowed in evidence where the statement was made while the witness was perceiving the event or condition, or immediately thereafter.[35] This exception requires two preconditions before admission. The following must be shown: (1) that the witness

clearly cannot recall what occured, and (2) that the statement will be used only for the purpose of stimulating the witness' memory.

Over time, courts have liberally interpreted this exception, admitting in evidence such documents as personal diaries, commercial records, letters, grand jury testimony, and even minutes from a board of directors' meeting. As always, the defendant has the right to inspect the written instrument and to cross examine the witness. It is feasible, as is the case with evidence admitted under the recorded recollection exception, that where such a statement has been recorded on a computer disc or tape, the information will be allowed under the present sense impression exception.

Statement Against Interest Exception

The statement against interest exception concerns a statement which, at the time it was made, was so contrary to the witness' financial or proprietary interest, or tended to subject him to civil or criminal liability rather than render invalid the claim of another against him, that a reasonable man would not have made the statement unless he believed it was true.[36]

In the prosecution of a computer crime, the accuracy and reliability of the computer generated evidence may be at issue. Testimony of certain employees of the company which owns and operates the computer could be crucial to a case. Where a financial officer or computer programmer testifies that the computer was constantly breaking down, the testimony could be admitted under the statement against interest exception. Likewise, the company's computer repair personnel could be summoned to testify concerning the frequency and type of repairs to which the computer was susceptible. However, statements against interest are not made "in a vacuum", and the possibility of testimony being solicited as the result of immunity from prosecution or plea-bargaining arrangement will be weighed accordingly.

OTHER CONSIDERATIONS CONCERNING ADMISSIBILITY OF EVIDENCE

As has been noted, evidentiary problems present a highly specialized variety of procedural problems that can arise in computer related crime cases. Beyond the somewhat abstract (though critical) questions of whether computer generated data can qualify for admission as the best evidence and under one or more allowable exceptions to hearsay, there exist other very real tactical problems in convincing the court that such evidence, once admitted, should be given great weight. The subsections which follow discuss the procedural aspects of successfully securing the court's confidence in computer generated data as evidence of the facts in dispute.

Laying the Proper Foundation

A proper foundation for the admission of computer records as evidence includes proof of the following:

- that any qualifying witness has proper credentials to be an expert witness on computer records;
- that the physical equipment and systems design are reliable;
- that the programs and operating personnel have had a history of overall system accuracy;
- that error detection and correction procedures have been continually carried out; and
- that audits made by independent agencies, if available, indicate that the records system is sound and has operated efficiently.[37]

A financial officer and a general manager may establish a proper foundation by testifying to their responsibility for maintaining company records and the procedures for such maintenance. The officers must testify that it was company practice to make entries into the computer within a reasonable time of the transaction. The prosecutor must be prepared to offer proof that only bona fide business records are placed in relevant files or programmed into the computer.

Where the records, or summaries of records, are specifically prepared for trial, the prosecutor must be prepared to identify the records and to offer testimony as to the means of preparation, and should make originals available to the defendant for his inspection. The prosecutor should also be prepared to weather any objections that such records were prepared "in contemplation of litigation" and therefore may contain a bias in their makeup or content that routine records kept in the normal course of business would not reflect. An inability to counter these objections could be fatal.

Conversely, the defendant could argue that computer security is lax and computer personnel are not properly screened, thereby casting some doubt as to the reliability of the prosecution's "proof". Again, the credibility of the underlying record, though otherwise admissible, is challenged.

An early case concerning the admissibility of computer evidence established that printout sheets of business records stored on electronic computer equipment would be admitted into evidence if it could be shown that the evidence was "relevant and material" to the prosecutor's case.[38] The prosecution would not have to identify, locate or produce as witnesses the persons who

made the entries in the regular course of business, if the following could be shown:

- that the entries were made in the regular course of business at or reasonably near the time of the transaction or event, and

- that the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and to justify its admission.

The primary two obstacles to establishing a proper foundation are the requirements of the business records exception to the hearsay rule, discussed above, and trustworthiness standards. As has been discussed, the business records exception requires that the computer records be shown to have been made in the regular course of business, at or near the time of the transaction, by a person with knowledge of the transaction. The prosecution must then show that the computer procedures which were employed in fact insure the reliability, accuracy and completeness of the records.

Other areas of concern to prosecutors when seeking to lay a proper foundation include the identity of computer hardware and software, the mode of preparation, time of preparation, and, of particular importance, the trustworthiness of the record. The trustworthiness requirement also entails a demonstration that the computer system in question protects against human error and mechanical breakdowns. The issue of demonstrating the trustworthiness of the record will be discussed in further detail below, because of its pivotal importance.

Trustworthiness of Computer Generated Records

The court must be satisfied that the overall preparation of computer records is surrounded by elements of accuracy, reliability and lack of motivation to falsify so as to remove any doubt concerning the propriety of admitting the records. In computer crime prosecutions, the prosecutor must anticipate inquiries into such areas of concern as the type of computer hardware or software that is standard in the industry at issue; the type of personnel recruitment, screening, training, rotation and security; and the type of input-output procedures employed. Good prosecutorial anticipation of and preparation for these inquiries may convince the court of the trustworthy nature of the records.

The areas of inquiry expand as the particular system is examined in greater detail. For example, if a time lag exists between manual and computerized recordation, is this a standard industry time lag? Further, what safeguards exist to protect against sabotage or error, and are the safeguards properly

implemented? Is the computer hardware programmed to detect errors? If so, is this part of the program routinely checked to insure that the programming for errors is functioning properly? In some industries, it is standard practice to intentionally input false data into the computer to check on the computer's error detecting capabilities. These considerations may be very important to establishing the trustworthiness and overall propriety of admitting the computer records in question.

In a now classic Federal prosecution, a doctor and several associates were charged with mail fraud for their part in devising a scheme to obtain payments from Blue Cross for services they did not render.[39] The prosecution presented the insurance company's director of service review as a qualifying witness to verify the computerization of information. This was done in an effort to introduce computer records of the company indicating payments made to participating physicians. However, the defense was able to elicit from the director that computer records are susceptible to the "GIGO" syndrome--"garbage in, garbage out". The prosecution then presented other company officials who testified as to error detection efforts and pretesting of computer programs for accuracy. The Federal appeals court affirmed the trial court's ruling that the prosecution had established the reliability of the records. The appeals court noted that the defendant failed to challenge the computer's mechanical or electronic capabilities, and the basic trustworthines of the system and data output were deemed to be established.

CONCLUSIONS

As will be discussed in the concluding chapter to this volume, few States at present have on their books statutes which define computer related crimes or which proscribe particular acts which involve the use of a computer or computer generated data. Nor does such legislation exist at the Federal level. As a consequence, the battle against computer related crime continues to be fought primarily by the analogous application of "traditional" laws, as discussed in the first chapter.

The evidence codes and criminal procedure statutes and case law in many jurisdictions pose significant tactical problems for the prosecutor seeking to convict the computer felon. Any discussion of the application of traditional criminal, civil and administrative law provisions in the non-traditional context of computer related crime would therefore be incomplete without an analysis of the procedural law issues--most of them evidentiary--that must be encountered and overcome in the process.

As has been noted, the record of reported cases of computer related crime prosecutions remains small, due in part to the comparative recency of the phenomenon itself and in part to the fact that computer related issues arise only peripherally in many

cases, the main holdings of which have to do with other issues of law or of fact. Regardless, the now growing body of case law in the area of computer related crime demonstrates the points of great relevance here. First, when litigating computer related issues per se, the evidentiary and other procedural law questions involved in these cases tend to be more determinative than do the substantive law questions. Second, the evidentiary and other procedural law hurdles that must be surmounted to sustain a successful prosecution for a computer related crime are indeed formidable and not easily overcome.

FOOTNOTES--EVIDENTIARY AND OTHER PROCEDURAL ISSUES

1. Computer Abuse and Criminal Law, Ed. H. Coughran (La Jolla Calif.: University of Calif., San Diego, 1976), pp. 40-41.
2. Computer Law: Evidence and Procedure, David Bender (New York: Matthew Bender and Co., 1980), Dec. 9.01(1), pp. 9-8,9-9.
3. New Federal Rules of Evidence, Rule 1006.
4. Transportation Co. v. Seib, 132 N.W.2d 871 (1965).
5. Otto G. Obermaier, "Special Aspects of Litigating White-Collar Criminal Cases", Litigation (ABA), Vol. 6, No. 3, Spring 1980, p. 13.
6. Uniform Photographic Copies of Business and Public Records Act.
7. King v. State ex rel. Murdock Acceptance Corp., 222 So.2d 393, 398 (1969).
8. 28 USC §1732.
9. United States v. Fendley, 552 F.2d 181 (1975).
10. Computer Crime--Criminal Justice Resource Manual (OJARS) (Washington, D.C.: U.S. Printing Office 1980), p. 355, Case No. 7336.
11. Martin v. Glenn's Furniture Co., Inc., 126 Ga. App. 692.
12. The New Federal Rules of Evidence Annotated, Paul F. Rothstein (Washington, D.C.: Bureau of National Affairs, Inc. 1975), p. 1.
13. 28 USC §1732.
14. New Fed. Rul. Evid., Rule 102.
15. Id., Rule 803(6).
16. Id., Rule 901(9).
17. Id., Rule 100(1).
18. United States v. DeGeorgia, 420 F.2d 889, 893, n. 11 (9th Cir. 1970).
19. August Bequai, Computer Crime (Lexington, Mass.: D.C. Heath & Co., 1978) (hereinafter cited as Bequai), p. 119.
20. 9 A.U.L.A. 598 (1965).

21. Neb. Rev. Stat., 25-12, 109 (1964).

22. State of Arizona v. Veres, 536 P. 2d 629 (1968).

23. Transport Indemnity Co. v. Seib, 132 N.W.2d 871, at 874 (1965).

24. Tex. Rev. Civ. Stat., art. 3737e (Supp. 1973).

25. Railroad Commission v. Southern Pacific Railroad Co. 468 S.W. 2d 125 (Ct. Civ. App. Tex. 1971).

26. Arnold D. Kamen & Co. v. Young, 466 S.W.2d 381 (Ct. Civ. App. Tex. 1971).

27. Colin Tapper, "Evidence From Computers", 8 Ga. L. Rev. 591 (1974).

28. Bequai, supra note 19, p. 126.

29. Id., p. 103.

30. 18 USC §3500(b).

31. 18 USC §3500(d).

32. 18 USC §3500(e).

33. United States v. Kelly, 349 F.2d 720 (1965).

34. New Fed. Rul. Evid., Rule 803(5).

35. Id., Rule 803(1).

36. Donnely v. United States, 228 U.S. 243 (1913).

37. Note, "Admissability of Computer Printouts," 52 N.C.L. Rev. 903, 93 (1974).

38. King v. State ex rel. Murdock Acceptance Corp., 222 So. 293.

39. United States v. Russo, 480 F.2d 1228 (6th Cir. 1973), cert. denied 414 U.S. 1157.

CHAPTER III: PRIVACY AND SECURITY ASPECTS

This chapter provides a state of the art review of statutes and executive orders which address the privacy and security aspects of computer related crime. Material presented in the text is supplemented by that which appears in Appendix "E".

Privacy issues arise in a computer context insofar as the law recognizes certain information which may be maintained on computers as confidential and affords legal protection against its misuse. The basis for such protection may be statutory, common law and/or constitutional. The information protected may pertain to individuals, to businesses (proprietary information), or to government itself (e.g., national security information). Privacy considerations give rise, in turn, to considerations of computer security, to the end of safeguarding computer systems and the integrity and confidentiality of information maintained within them.

The first significant recognition, historically, of a legal right to privacy was that of then Harvard law professor (later Supreme Court Justice) Louis Brandeis, who in 1890 in a law review article co-authored with Samuel Warren wrote of "the right of the individual to be let alone."[1] Thirty-eight years later, in a now famous dissent to a Supreme Court opinion holding wiretapping to be outside the reach of the Fourth Amendment's limitations on search and seizure, Justice Brandeis characterized this right as "the most comprehensive of rights and the most valued by civilized man."[2]

Since that time, the law has come to recognize a right to privacy on a number of levels. Justice Brandeis' dissenting opinion in the case noted above is now the law of the land. Most States by far, moreover, recognize the right of an individual to sue another for invasion of privacy, though such a suit to be successful will require a showing (1) that the disclosure would be highly offensive to a reasonable person, (2) that the information disclosed was truly private, and (3) that the information was made publicly known.[3]

The focus of this chapter is, however, not constitutional or common law, but rather statutory and administrative law, with regard to which a number of points should be noted at the outset. First, there is not merely one way but, rather, a number of alternative ways in which an informational privacy or computer security statute may have relevance to computer related crime. The following section will describe five broad statutory purposes which existing Federal legal provisions of possible applicability to computer related crime may serve. Particular statutes and regulations that fall into each category are then identified.

Second, it will be seen that there are relatively few statutes and administrative issuances in this area, and only certain of these are relevant on the basis of offering criminal penalties by which computer related acts may be prosecuted. Third, while related case law is noted throughout, it will be seen that generally speaking there has been a paucity of litigation in this area. (One may note, in particular, the number of those statutes containing criminal penalties for unlawful disclosures of information under which there have been no reported prosecutions.) Fourth, a central reason for the lack of reported criminal and civil case laws is the recency of the various statutes.

With regard to the sparseness of prosecutions, this is somewhat predictable. (Consider the absence of prosecutions, for example, under the Trade Secrets Act, adopted in 1948). The recency of statutory and administrative law in the area of computer security and informational privacy is striking. Of the 20 Federal statutes and executive orders identified in the following section, 11 have come into existence since 1970, nine since 1974, six since 1976, and four since 1978. (The most significant computer security provision was promulgated only two years ago.)

Finally, this chapter is intended to address privacy and security aspects of computer related crime. While much of informational privacy law may be relevant in one way or another to the investigation and prosecution of computer related crime, it should be noted that the relevance of computer security law is essentially and almost exclusively related to the prevention of computer related crime.

The following sections address two primary areas--Federal statutes and State statutes in this area. A last section will summarize the chapter and present conclusions.

FEDERAL STATUTES ON PRIVACY AND SECURITY

There are a substantial number of Federal statutes and executive orders pertinent to privacy and security aspects of computer related crime. The most significant of these are presented in Table 2.1. Statutes and executive orders cited in Table 2.1 are classified into five categories. These are as follows:

- provisions prescribing criminal penalties for unlawfully accessing information, coded in the Table with the letter "A";

- provisions prescribing criminal penalties for unlawfully disclosing information, coded with the letter "B";
- provisions prohibiting disclosure but providing no criminal penalties--including simple prohibitions or restrictions upon disclosure, non-disclosure as a condition for Federal funding, provisions for civil liability, provisions for injunctions to prevent disclosures, and provisions for administrative sanctions; coded with the letter "C";
- provisions requiring safeguarding of information, coded with the letter "D"; and
- provisions affording access for law enforcement purposes to otherwise unavailable information, coded with the letter "E".

Since several of the key Federal statutes in this area are germane to two or more of these five categories, some statutes, (for example, the Privacy Act) will fall within two or more groupings. However, in these instances different subsections of the statute will address these separate purposes.

Following Table 2.1 is a discussion of each of these five categories, and a citation and summary analysis of the applicable sections of each of the statutes/executive orders listed in the Table. Provisions affecting governmental records are grouped together and presented first, followed by those provisions which only affect private sector records.

The following is a discussion of each of the categories noted in Table 2.1.

TABLE 2.1

Table of Federal Statutes and Executive Orders Pertinent to Privacy and Security Aspects of Computer Related Crime

	CITATION	RECORDS EFFECTED	TITLE OF THE STATUTE	TYPE OF PROVISION
1	5 U.S.C. 552	G	Freedom of Information Act	E
2	5 U.S.C. 552a	G	The Privacy Act of 1974	A-B-D-E
3	12 U.S.C. 3401 et seq.	P	Right to Financial Privacy Act	C-E
4	13 U.S.C. 9214	G	Census Act	B
5	15 U.S.C. 1666a	P	Fair Credit Billing Act	C
6	15 U.S.C. 1681	P	Fair Credit Reporting Act	A-B-C-E
7	15 U.S.C. 1693	P	Electronic Funds Transfer Act	A
8	18 U.S.C. 641	G	Embezzlement and Theft Prohibition	A
9	18 U.S.C. 793, 794	G	Espionage Acts	A-B
10	18 U.S.C. 1343	G-P	Wire Fraud Prohibition	A
11	18 U.S.C. 1905	G	Trade Secrets Act	B
12	20 U.S.C. 1232g	P	Family Educational Rights and Privacy Act	C
13	26 U.S.C. 6103, 7213, 7216, 7217	G-P	Internal Revenue Code on Confidentiality	A-B-C-D-E
14	26 U.S.C. 7609	P	Special Procedures for Third Party Summons	C
15	42 U.S.C. 408 (h)	G	Confidentiality of Social Security Numbers	B
16	42 U.S.C. 5103 (b)(2)(e)	G	Confidentiality of Child Abuse Information	C
17	44 U.S.C. 3101-3315	G	Records Management by Federal Agencies	D
18	44 U.S.C. 3508	G	Interagency Information Exchanges	B-C
19	E.O. 10865	G	Safeguarding Classified Information Within Industry	C-D
20	E.O. 12065	G	Rules Governing Classified Information	C-D-E

KEY: G = Government Records Covered
P = Private Sector Records Covered
A, B, C, D, E = Categories of Statutes Described in the Preceding Text

Category A--Statutes Providing Criminal Penalties for Unlawfully Accessing Information

There are several key Federal statutes which provide criminal penalties for unlawfully obtaining information. Since information stored within a computer may be the target of the criminal act these provisions may be increasingly relevant. These include the following:

- Privacy Act (5 USC §552 a (i) (3)--The Privacy Act of 1974 governs the collection, maintenance, use and dissemination of individually-identifiable information contained in Federal agency records systems, and provides for access by an individual to his or her own records. The Act makes it a misdemeanor subject to a fine of not more than $5,000 for any person to knowingly and willfully request or obtain records under false pretenses. There have thus far been no criminal prosecutions under this or under either of the other two criminal penalty provisions of the Act.

- Embezzlement or Theft of Government Property (18 USC §641)--This statute provides criminal penalties for the embezzlement or theft of any record, voucher, money, or thing of value belonging to the United States, or thing made or being made under contract for the United States. The property in question must belong to the United States and the individual prosecuted must have had knowledge that it did. The Second Circuit has held that this statute is not limited in its coverage to tangible property, and is violated by the sale of information.[4]

- Espionage Act (18 USC §793 (a), (b), (c), (g))--Espionage Act provisions make unlawful specified activities undertaken for the purpose of obtaining information with respect to the national defense, and with an intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. The term "national defense" in the context of these provisions has been interpreted as a generic concept of broad connotation.[5]

- Wire Fraud Statute (18 USC §1343)--This statute provides criminal penalties for fraudulently obtaining or attempting to obtain money or property through the use of wire, radio or television communications crossing State lines. The Fourth Circuit, on the facts of a recent case, held a computer system to be property within the meaning of this statute and affirmed a conviction under this statute for the fraudulent retrieval of information from a computer system without authorization.[6]

- Soliciting Federal tax information (26 USC § 7213 (a)(4))--This provision, amended to the Tax Code in 1978, subjects to criminal prosecution any person who willfully offers any item of material value in exchange for any tax return or tax return information, and who receives as a result of such solicitation any such return or return information. There have thus far been no reported prosecutions.

- Fair Credit Reporting Act (15 USC §1681 a)--This provision of the Fair Credit Reporting Act provides criminal penalties for obtaining information on a consumer from a reporting agency under false pretenses. The defendant must have acted knowingly and willfully. The Ninth Circuit has held that in addition to criminal prosecution, the statute permits a private suit by the individual on whom the information was unlawfully obtained.[7]

- Electronic Funds Transfer Act (15 USC §1693 n)--This provision of the Electronic Fund Transfers Act provides criminal penalties for various forms of misuse of any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument. The statute defines debit instrument as a card, code, or device, other than a check, draft or similar paper instrument, by the use of which a person may initiate an electronic funds transfer. The purpose of the Act as a whole is to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems; its primary objective is the provision of individual consumer rights.

Category B--Statutes Providing Criminal Penalties for Unlawfully Disclosing Information

The following Federal statutes provide a criminal penalty for unlawfully disclosing, as distinguished from obtaining, information. Such criminal sanctions may be applicable to acts by technical custodians of information (e.g., data processing personnel) or by other persons having indirect access to information stored in an automated environment.

- Privacy Act (5 USC §552 a (i)(1), (m), (b))--Paragraph (i)(1) of the Privacy Act makes it a misdemeanor subject to a fine of not more than $5,000 for a Federal agency officer or employee to knowingly and willfully disclose information except as permitted by the Act. Contractors, as defined in paragraph (m), are likewise subject to the Act's criminal penalties. The 11 specific conditions under which disclosure of information is permitted by the Act are delineated in paragraph (b). There have thus far been nc criminal prosecutions under

this or either of the other two criminal penalty provisions of the Act.

- Disclosure of census data (13 USC §§9, 214)--This provision stipulates that no Commerce Department officer or employee may permit anyone other than the sworn officers and employees of the Department to examine any individual census report; it further stipulates that individual census reports shall be immune even from legal process. Contravention of this statute by present or former Commerce Department employees subjects them to criminal penalties under 13 USC §214.

- Espionage Act (18 USC §§793(d), (e), (f), (g), 794)--These provisions of the Espionage Act provide criminal penalties for specified acts of transmitting, losing, gathering or delivering national defense information with an intent to advantage a foreign nation or injure the United States. The information need not be classified.[8]

- Trade Secrets Act (18 USC §1905)--The Trade Secrets Act subjects officers and employees of the United States to fines of not more than $1,000 or imprisonment for not more than one year, or both, and to removal from office or employment, for any disclosure not authorized by law of trade secret information to which one is privy by virtue of his or her position. There have been no reported prosecutions under the Act. Additionally, it has been held that an individual or corporation has no right under the Act to initiate a private suit to prevent disclosures of information by Federal employees in violation of the Act.[9]

- Disclosing Federal tax return information (26 USC §7213 (a))--This provision subjects the unlawful disclosure of tax returns and tax return information to fines of not more than $5,000, or imprisonment for not more than five years, or both, together with the costs of prosecution. (Regarding those instances where the disclosure of such information is authorized by law, see 21 USC §6103 and the section entitled Provisions Affording Access for Law Enforcement Purposes, below.)

- Redisclosure of privileged information (44 USC §3508)--This provision provides, in pertinent part, that if information obtained in confidence by a Federal agency is released by that agency to another Federal agency, all the provisions of law--including penalties which relate to the unlawful disclosure of information--apply to the officers and employees of the agency to which information is released, to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

- Fair Credit Reporting Act (15 USC §1681 (r), (s))--The Fair Credit Reporting Act, in subsection (r), stipulates that any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined not more than $5,000, or imprisoned for not more than one year, or both. Subsection (s) provides that enforcement shall be by the Federal Trade Commission.

- Disclosure of prepared income tax data (26 USC §7216)--This provision makes it a misdemeanor for an income tax preparer to disclose, except as otherwise authorized by law, information furnished to him or her in connection with the preparation of a Federal income tax return.

Category C--Provisions Impacting on Disclosure But Entailing No Criminal Penalties

The following Federal laws may impact on the disclosure of information (which could include computer data) but impose no criminal penalties.

- Confidentiality of child abuse records (42 USC §5103 (b) (2) (E))--This provision requires that, in order for a State to qualify for Federal financial assistance in developing, strengthening, and carrying out child abuse and neglect prevention and treatment programs, the State must provide for methods to preserve the confidentiality of all records so as to protect the rights of children, and their parents or guardians.

- Disclosure of classified information (E.O. 12065)--Except as provided in the Atomic Energy Act of 1954, as amended, this Executive Order constitutes the sole standard and basis for classifying information. Section 5-5 of the Order provides for administrative sanctions. Federal Government officers and employees shall be subject to such sanctions for knowing and willfull violation of any provision of the Order, including classifying information in violation of the Order, or for disclosing without authorization, properly classified information. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or any other sanction in accordance with applicable law and agency regulations.

- Right to Financial Privacy Act (12 USC §3401 et seq.)--Section 3417 of the Right to Financial Privacy Act provides that any agency or department of the United States or financial institution obtaining or disclosing financial records of information contained therein in violation of the Act shall be liable to the customer to whom such records relate. It also provides in certain instances for disciplinary action against Federal Government officers or employees so involved. Section 3418 provides that a customer may also seek an injunction to require that the procedures of the Act are complied with.

- Family Educational Rights and Privacy Act (20 USC §1232 g)--The Family Educational Rights and Privacy Act conditions Federal funding of educational institutions and agencies on (1) their permitting parents of students access to the educational records of their children, and (2) their otherwise limiting access to such records to those specified in the Act. Enforcement of this provision is solely in the hands of the Secretary of Education; no private remedy is granted under the statute.[11]

- Disclosure of Federal income tax return (26 USC §7217)--By this provision, a taxpayer may bring a civil action for damages in Federal court against any person who knowingly or negligently has disclosed that taxpayer's tax return or return informaiton, other than as authorized or in good faith understood to be authorized by 26 USC §6103.

Category D--Provisions Requiring Safeguarding of Information

The following Federal statutes require that certain information be safeguarded and may be of possible applicability to computer related crime cases.

- Privacy Act (5 USC §552 a (e) (10))--The Privacy Act of 1974, in one of several agency requirements enumerated in paragraph (e), stipulates that an agency that maintains a system of records shall establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. (Paragraph (e) (10).

- Tax Reform Act of 1976 (26 USC §6103 (p)(4-8))--These provisions of the Tax Reform Act of 1976 require that any Federal agency, body, or commission and the General Accounting Office, as a condition for receiving tax returns or return information, provide safeguards for the confidentiality of such information, to the satisfaction of the Secretary of the Treasury. The provisions similarly require that States adopt provisions of law to safeguard Federal tax return information.

- Safeguarding against unauthorized removal or destruction of records (44 USC §§3105, 3106)--These provisions require, among other things, the establishment by Federal agencies of safeguards against the removal or loss of necessary records (§3105) and notification to the Administrator of the General Services Administration and, when appropriate, to the Attorney General in case of actual or forseeable unlawful removal or destruction of records (§3106).

- Classification of information (E.O.10865)--This Executive Order, in pertinent part, provides that the heads of agencies designated in the Order prescribe regulations for the safeguarding of classified information within key industries. The Order states that such regulations shall, so far as possible, be uniform and provide for full cooperation among the agencies concerned.

- Controlling access to classified information (E.O. 12065 §4)--Section 4 of this Executive Order provides for the safeguarding and, in particular, the controlling of access to classified information.

Category E--Statutory Provisions Allowing Access for Law Enforcement Purposes Only

Several provisions of Federal law allow access to otherwise confidential information by law enforcement. These may be relevant in connection with the detection and/or prosecution of computer related crimes.

- Exceptions under Privacy Act USC §552)--The Privacy Act of 1974's provision that information not be disclosed without the written consent of the individual affected is subject to 11 exceptions. These include disclosure (1) for a routine use [12] [a use compatible with the purpose for which the information was collected; routine uses are required to be specified in the Federal Register], (2) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought,[13] and (3) pursuant to the order of a court of competent jurisdiction.[14]

- Disclosure of Federal tax information (26 USC §6103)--This provision in paragraphs (c) through (o) delineates

the persons to whom, and the purposes for which and conditions under which tax returns and return information may be disclosed. Pertinent to this chapter are paragraphs (h) and (i), which concern disclosures to Federal officers and employees (including those of the Department of Justice), for, respectively, purposes of tax administration and the administration of Federal laws not relating to tax administration.

- Disclosure of otherwise classified information (E.O. 12065)--Section 5-505 of this Executive Order requires that agency heads report to the Attorney General any evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

- Disclosure of bank records (12 USC §3401 et seq.)--The Right to Financial Privacy Act provides that bank records may be obtained by Government authorities, but only in accordance with one of five specified procedures--customer authorization, administrative subpoena, judicial subpoena, formal written request, or search warrant. The Act sets forth the necessary conditions and procedures for each, including the manner in which notice and a right to be heard are to be afforded the depositor with each of the first four.[15]

- Disclosure of consumer credit information (15 USC §1681)--The Fair Credit Reporting Act provides in Subsection b(1) that a consumer reporting agency may furnish to a Government agency identifying information with respect to any consumer, limited to his name, address, former addresses, places of employment, or former places of employment.[16]

- Judicial order for educational records (20 USC §1232 g)--Among the limited and specified exceptions to the confidentiality of educational records provided for in the Family Educational Rights and Privacy Act is an exception under 20 USC §1232 g (b)(2)(B) for information furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.[17]

- Investigatory Records under Freedom of Information Act (5 USC §552)--The Freedom of Information Act requires that Federal agency records be made available to any person making a proper request. However, the Act specifies nine categories of records which may be withheld at the reasonable discretion of an agency. One of these

nine is "investigatory records compiled for law enforcement purposes".[18] These can be withheld only to the extent that production of such records would (a) interfere with enforcement proceedings,[19] (b) deprive a person of a right to a fair trial or an impartial adjudication, (c) constitute an unwarranted invasion of personal privacy,[20] (d) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, disclose confidential information furnished only by the confidential source,[21] (e) disclose investigative techniques or procedures, or (f) endanger the life or physical safety of law enforcement personnel."

STATE STATUTES PROVIDING FOR CONFIDENTIALITY OF COMPUTERIZABLE INFORMATION

A total of 44 of the 50 States have statutes on their books which provide for the confidentiality of one or more categories of computerizable information. In all, over 150 such statutes exist. Table 2.2, below, indicates the eight major groups into which such statutes fall and the number of statutes which research suggests fall in each group nationwide, as of the time of this writing.

CONCLUSIONS

The concern in informational privacy law is not specifically computers, but information. While the treatment of informational privacy law herein has been limited to provisions affecting computerizable information, the scope of these provisions extends generally to all forms of information--whether or not computerized. Where information is maintained on computers, these provisions may be relevant to the investigation and/or prosecution of computer related crime in one or another of several ways. As we have seen, certain provisions may be relevant to prosecution in that they provide criminal penalties for unlawfully obtaining or disclosing information. Other provisions may be relevant to both investigation and prosecution in that they afford access for law enforcement purposes to otherwise unavailable information or they afford control for law enforcement purposes over otherwise available information. Certain other important disclosure-prohibiting provisions have also been included though they entail no criminal penalties.

TABLE 2.2

Number and Types of State Statutes Governing Confidentiality of Computerizable Information

CATEGORY OF INFORMATION	NUMBER OF STATUTES	NUMBER OF STATES
1. Medical Records	15	31
2. Financial Records	19	29
3. Tax Records	24	25
4. Criminal Justice Records	14	21
5. Privacy Acts	10	11
6. Trade Secret Information	8	10
7. Educational Records	8	8
8. Other	10	15

Full titles and citations of all of the State statutes in each of the above eight categories are included elsewhere in this volume, together with notations as to whether any court cases have been reported with regard to each. (See Appendix "E", below.)

As we have seen, the law recognizes a privacy interest in certain types of information having to do with individuals, with businessses (e.g., trade secrets), and with Government itself (e.g., national security information). To the extent such information is maintained on computers, the state of informational privacy law generally becomes relevant. In this context, privacy considerations in turn give rise to considerations of computer security, the object of which is the safeguarding of computer systems and of the integrity and confidentiality of information maintained therein. Computer security law, in contrast to informational privacy law, is concerned specifically with computers, and relevant not so much to the investigation and prosecution of computer related crime, as to its prevention.

As time goes on, Federal and State level privacy and security statutes governing computerized information and computer systems will doubtless be more heavily relied upon to support computer related crime prosecutions. To date, however, this has not been the case.

The total number of computer privacy and security provisions cited is significant. However, the number of relevant Federal statutes is only 20 and the 150 State statutes cited, while not purporting to be fully inclusive, do span all topical areas in all 50 States. Moreover, only certain of the statutes cited entail criminal penalties by which computer related acts may be prosecuted. While related case law is noted in the footnotes to this chapter, generally speaking, there has been very little litigation in this area. One should note, in particular, that under most of the statutes containing criminal penalties for unlawful disclosure there have been no reported prosecutions. Clearly, the law is in a state of evolution in this area.

Computer security provisions, as distinguished from broad informational privacy laws, are of very recent origin and of even more limited applicability. As previously noted, the fundamental relation of computer security law to computer related crime is essentially preventive rather than investigative or prosecutive. Computer security law is also essentially administrative, as opposed to statutory. A significant number of purely administrative regulations and guidelines exist which have been promulgated by various agencies of Government. As non-compliance with these administrative directives does not lead to criminal sanctions, they have not been included here.

FOOTNOTES--PRIVACY AND SECURITY ASPECTS OF COMPUTER RELATED CRIME

1. Warren and Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890).

2. Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J., dissenting).

3. See Restatement (Second) of Torts §652D (1965) Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

4. United States v. Guiard, 601 F.2d 69 (2nd Cir. 1979).

5. United States v. Semaan, 594 F.2d 1215 (8th Circ. 1979).

6. United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

7. Hansen v. Morgan, 582 F. 2d 1214 (9th Cir. 1978).

8. United States v. Lee, 589 F.2d 980 (9th Cir. 1979); Edgar and Schmidt, The Espionage Statutes and Publication of Defense Information, 73 COLUM. L. REV. 929 (1973).

9. Chrysler Corp. v. Brown, 44 U.S.W. 4434 (1979); see generally Department of Justice, Office of Information Law and Policy, Statement Concerning the Supreme Court Decision in Chrysler v. Brown, 44 U.S.L.W. (April 18, 1979) (6/15/79).

10. Mayer, S., Privacy and the SSN: Section 1211 of the Tax Reform Act of 1976, 6 RUTGERS J. OF COMPUTERS AND THE LAW 221 (1978).

11. Girardier v. Webster College, 563 F.2d 1267 (8th Cir. 1977).

12. Harper v. United States, 423 F. Supp. 192 (D.C. S.C. 1976); Burley v. United States Drug Enforcement Administration, 443 F. Supp. 619 (M.D. Tenn. 1977); Stiles v. Atlantic Gas Light Co., 453 F. Supp. 798 (N.D. Ga. 1978).

13. United States v. Collins, 596 F.2d 166 (6th Cir. 1979).

14. Stiles v. Atlanta Gas Light Co., 453 F. Supp. 798 (N.D. Ga. 1978).

15. Palmer and Palmer, Complying with the Right to Financial Privacy Act of 1978, 96 THE BANKING L.J. 196 (March 1979).

16. Federal Trade Com. v. Manager, Retail Credit Co., Miami Branch Office, 515 F.2d 988 (D.C. Cir. 1975): United States v. Pintorieri, 379 F. Supp. 332 (D. N.Y. 1974); Laufman v. Oakley Building & Loan Co., 72 F.R.D. 116 (D. Ohio 1976); see Re TRW, Inc., 460 F Supp. 1007 (D. Mich. 1978); but see Application of Credit Information Corp., 457 F. Supp. 969 (D. N.Y. 1978).

17. T v. Johnston, 74 F.R.D. 498 (D. Miss. 1976); Reeg v. Fetzer, 78 F.R.D. 34 (D. Okla. 1976).

18. See Rural Housing Alliance v. Department of Agricultrue, 498 F.2d 73 (D.C. Cir. 1974); Williams v. IRS, 479 F.2d 317 (3rd Cir. 1973).

19. NLRB v. Robbins Tire Rubber Co., 437 U.S. 214 (1978); United States v. Murdock, 548 F.2d 599 (5th Cir. 1977); Title Guarantee v. NLRB, 534 F.2d 484 (2d Cir. 1976); Climax Molybdenum Co. v. NLRB, 539 F.2d 63 (10th Cir. 1976); Roger J. Au and Son., Inc. v. NLRB, 538 F.2d 80 (3d Cir. 1976); New England Medical Center Hospital v. NLRB, 548 F.2d 377 (1st Cir. 1976); AMF Head Division of AMF v. NLRB, 564 F.2d 374 (10th Cir. 1977).

20. See Deering Milliken v. Irving, 458 F.2d 1131 (4th Cir. 1977); Moroscio v. Levy, 569 F.2d 1000 (7th Cir. 1977).

21. See Nix v. United States, 572 F.2d 998 (4th Cir. 1978); Evans v. Dept. of Transportation of United States, 466 F.2d 821 (5th Cir. 1971).

CHAPTER IV: COMPUTER RELATED CRIME LEGISLATION

Though most States have to date not adopted statutes that specifically address computer related crime, to date a growing minority have done so. These include Arizona, California, Colorado, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, and Utah. At the Federal level, Senator Abraham Ribicoff (D-Conn.) first introduced the Federal Computer Systems Protection Act (S.240) in 1977. (As of the close of the 96th Congress, the Ribicoff bill had yet to be enacted. It will reportedly be reintroduced in the 97th Congress, but as of this writing this has not yet occurred.)

STATE LEGISLATION

Although there has been some controversy concerning the actual definition of "computer crime," the States listed above have in different ways attempted to define the parameters of this term. For example, the Arizona bill defines types of computer crimes, whereas the California act defines the extent of the protected computer hardware to include programmable pocket calculators. Proposed legislation which was defeated in Connecticut encompassed trade secrets within its terms, as does the enacted Florida statute.

Legislative proposals in the area of computer related crime generally address the fraudulent use of, or improper access to, the computer hardware or software. The more progressive bills have also addressed the need for establishing a computer privacy law. Still other forms of computer related crime bills are directed at computer security, and attempt to provide adequate protection for the integrity and confidentiality of personal and other sensitive information. Property rights with regard to computer programs and penalties for violating such rights have been addressed in unsuccessful legislation.

Appendix "F" to this volume lists the title and citation of recently proposed and/or enacted computer related crime bills at the State level. This compilation, though current as of this writing, is of course subject to change. Given the fact that bills were pending in several States at the time that this review was undertaken, it can be expected that the 1981 legislative session(s) may change this picture significantly.

FEDERAL LEGISLATION

In June 1977, Senator Ribicoff introduced for the first time in the Senate the Federal Computer Systems Protection Act. The bill encompassed all intentional alterations or destruction of any kind or any part of a computer system or network. "Property"

was defined within the bill to include all "electronically produced data".[1]

Because that session of Congress ended with no action on the bill, Senator Ribicoff subsequently introduced the Federal Computer Systems Protection Act of 1979 (S.240), which included some minor changes to earlier versions of the proposed statute. An identical bill was introduced in the House. These Federal bills addressed four areas of computer related criminal activity--fraudulent records or data; unauthorized use of data; alteration or destruction of data; and theft of products, services or data associated with computers or information systems.

The proposed legislation (S.240) would have proscribed the use of, or attempt to use, a computer with the intent to defraud or to obtain property falsely, as well as theft or embezzlement of property. The bill was before the Subcommittee on Criminal Justice of the Senate Judiciary Committee as of November 1980. Whether it will be reintroduced in the 97th Congress and if so, what modifications it will feature over the previous version, remains uncertain. However, further attempts to enact such legislation at the Federal level will doubtless continue.

Appendix "G" to this volume presents a brief summary of the highlights of S.240 as it appeared in the last Congress. The full text of the bill has been widely circulated and has been commented upon extensively in the literature.[2]

FOOTNOTES

COMPUTER CRIME LEGISLATION

1. The bill when first introduced was known as S. 1766. A House version, H.R. 8421, was introduced by Congressman Charles Rose (D-N.C.).

2. "On Computer Crime (Senate Bill S. 240)", John K. Taber, Computer/Law Journal, Vol. 1, No. 3, Winter 1979, p. 532, fn. 88, citing Gruenberger, "What's In a Name?", Datamation, May, 1979, at 230.

BIBLIOGRAPHY

Akin, Richard H. The Private Investigator's Basic Manual. Springfield, Illinois: Charles C. Thomas, 1976.

Allen, Brandt. "Embezzler's Guide to the Computer." Harvard Business Review (July-August 1975).

Allen, Brandt R. "Computer Fraud." Financial Executive 39 (May 1971). p.38-43.

Anderson, Ronald A., and Kumpf, Water A. Business Law. Cincinnati, Ohio: South-Western Publishing Co., 1972.

Awad, Elias, M., and Data Processing Management Association. Automatic Data Processing--Principles and Procedures. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1973.

Barmash, Isadore, ed. Great Business Disasters: Swindlers, Bunglers, and Frauds in American Industry. Chicago: Playboy Press, 1972.

Baruch, Hurd. Wall Street Security Risk. Washington, D.C.: Acropolis Books, 1971.

Becker, Jay. The Investigation of Computer Crime. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Becker, Robert S. The Data Processing Security Game. New York: Pergamon Press, 1977.

Benson, George C.S., and Engerman, Thomas S. Amoral America. Stanford, California: Hoover Institution Press, 1975.

Bequai, August. Computer Crime. Lexington, Massachusetts: D.C. Heath, 1977.

Bequai, August. White Collar Crime: A Twentieth Century Crisis. Lexington, Massachusetts: D.C. Heath, 1978.

Bequai, August. Organized Crime: The Fifth Estate. Lexington, Massachusetts: D.C. Heath, 1979.

Bequai, August. The Cashless Society: EFTS at the Crossroads. New York: John Wiley & Sons, 1980.

Bequai, August. "Litigation under the EFTS." Federal Bar News 23 (June 1976). p.174-177.

Bequai, August. "Crooks and Computers." Trial Magazine 12 (August 1976). p.48-53.

Bequai, August. "Wanted: The White Collar Ring." Student Lawyer 5 (May 1977). p.44-48.

Bequai, August. "The Binary Burglars." Student Lawyer 5 (February 1977). p.18-24.

Bequai, August. "White Collar Plea Bargaining." Trial Magazine 13 (July 1977). p.38-43.

Bequai, August. "Legal Problems in Prosecuting Computer Crimes." Security Management 21 (July 1977). p.26-27.

Bequai, August. "White Collar Muggers Have Reason to Feel Safe." Barrister 4 (Summer 1977). p.26-29.

Bequai, August. "The Forty Billion Dollar Caper." Police Chief XLIV (September 1977). p.66-68.

Bequai, August. "Computer Fraud: An Analysis for Law Enforcement." Police Chief XLIII (September 1976). p.54-57.

Bequai, August. "The Cashless Society: An Analysis of the Threat of Crime and the Invasion of Privacy." University of Utah Journal of Contemporary Law 3 (Winter 1976). p.46-60.

Bequai, August. "The Electronic Criminal." Barrister 4 (Winter 1977). p.8-12.

Bequai, August. "The Impact of EFTS on Our Criminal Justice System." Federal Bar Journal 35 (Summer 1976). p.190-205.

Bequai, August. "Prosecutorial Decision-Making." Police Law Quarterly 4 (October 1974). p.34-42.

Binns, James. "The Internal Auditor's Role in Questioning Fraud Suspects, Part I." The Magazine of Bank Administration (October, 1977).

Blake, Ian F.; and Walker, Bruce J. Computer Security and Protection Structures. Stroudsburg, Pennsylvania: Dowden, Hutchinson & Ross, Inc., 1977.

Canadian Institute of Chartered Accountants. Computer Audit Guidelines and Computer Control Guidelines. Toronto, Canada, 1970.

Carroll, John M. Computer Security. Los Angeles: Security World Publishing Co., Inc., 1977.

Comptroller General of the United States, Report to the Congress. Computer Related Crimes in Federal Programs. U.S. General Accounting Office, 1976.

Coughran, Edward H. "Prosecuting Computer Abuse." Criminal Justice Journal Vol. 1 (1978).

Davis, Keagle W., Mair, William C., and Wood, Donald R. Computer Control & Audit. The Institute of Internal Auditors, Inc., 1976.

Finch, James H., "Espionage and Theft Using Computers." Assets Protection Vol. 2 No. 1. (1976).

Glick, Rush G. and Newsom, Robert S. Fraud Investigation. Springfield, Illinois: Charles C. Thomas, 1974.

Hagen, Roger E. The Intelligence Process and White-Collar Crime. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Harris, Louis, and Associates, Inc., and Westin, Dr. Alan F. A National Opinion Research Survey of Attitudes Toward Privacy, (1978).

Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1977.

Hoyt, Douglas. Computer Security Handbook, New York: Macmillan Information, 1973.

IBM. Data Security and Data Processing Volume 5, Study Results. IBM (No. G320-1375).

Inbau, Fred E., Moessens, Andre A., and Vitullo, Louis R. Scientific Police Investigation. Philadelphia: Chilton Book Co., 1972.

Jancura, Elise G. and Berger, Arnold H. Computers, Auditing and Control. Philadelphia: Auerbach, 1973.

Kirk, Paul L. and Thorton, John I., editors. Crime Investigation (second edition). New York: John Wiley & Sons, 1974.

Krauss, Leonard I. SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. New York: AMACOM, American Management Associations, 1973.

Larsen, Kent, S., ed,. Privacy, A Public Concern, A Resource Document (August 1975) (GPO).

Leininger, Sheryl, editor. Internal Theft: Investigation and Control, An Anthology. Los Angeles: Security World Publishing Co., Inc., 1975.

Liebholz, Stephen and Wilson, Louis. Users Guide to Computer Crime. Chilton Book Co., 1974.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, New Jersey: Prentice-Hall, 1973.

Mayer, Stephen, "Privacy and the Social Security Number: Section 1211 of the Tax Reform Act of 1976." Rutgers Journal of Computers and the Law 221 1978.

Mettler, George B. Criminal Investigation. Boston: Holbrook Press, Inc., 1977.

O'Brien, David M. "Privacy and the Right of Access: Purposes and Paradoxes of Information Control." 30 Administrative Law Review 45 1978 (excellent reference discussing the balancing process between FOIA and the Privacy Act of 1974).

O'Hara, Charles E. Fundamentals of Criminal Investigation (second edition). Springfield, Illinois: Charles C. Thomas, 1970.

O'Neill, Robert. Investigative Planning. Report prepared for Battelle Law and Justice Study Center, Seattle, Washington, 1978.

Osborn, Albert S. Questioned Document Problems. Albany, New York: Boyd Printing Company, 1944.

Parker, Donn B. Computer Abuse Assessment. A Stanford Research Institute report prepared for the National Science Foundation, Washington, D.C., 1975.

Parker, Donn B. Crime by Computer. New York: Charles Scribner's Sons, 1976.

Ralston, Anthony, ed. and Meek, Chester L., asst. ed. Encyclopedia of Computer Science. New York: Petrocelli/Charter, 1976.

"Records, Computers and the Rights of Citizens." HEW Report of the Secretary's Advisory Committee on Automated Personal Data Systems.

Rule, James B. "Electronic Funds Transfer and Federal Privacy Policy." 18 Jurimetrics Journal 56 1977.

Ruthberg, Zella G., ed. Audit and Evaluation of Computer Security. U.S. Dept. of Commerce, National Bureau of Standards, (NBS No. 500-19), 1977.

Shaw, Paul D. "Investigative Accounting." Assets Protection Vol. 3 No. 1 (Spring 1978).

SRI International. Computer Crime--Criminal Justice Resource Manual. Produced under contract to the National Criminal Justice Information and Statistics Service (1979)(GPO).

The Institute of Internal Auditors. Systems Auditability and Control Study. A three part report prepared by Stanford Research Institute under a grant from IBM Corporation. The Institute of Internal Auditors, Inc., 1977.

The Investigation of White-Collar Crime: A Manual for Law-Enforcement Agencies. Produced by Battelle Law and Justice Study Center under Grant No. 76-Ta-99-0011. The manual may be ordered from: U.S. Government Printing Office, Washington, D.C. 20402, Stock No. 027-000-00507-1.

Vandiver, James V. "Forensic References." Assets Protection Vol. 2. No. 4 (Winter 1977).

VanTassel, Dennis. Computer Security Management. Englewood Cliffs New Jersey: Prentice-Hall, Inc., 1972.

Walker, Bruce J. and Blake, Ian F. Computer Security and Protection Structures. Stroudsberg, Pennsylvania: Dowden, Hutchinson & Ross, Inc., 1977.

Westermeier, J.T. "The Privacy Side of the Credit Card." 23 American University Law Review 183 1973.

Whiteside, Thomas. Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. New York: Thomas Y. Crowell Company, 1978.

INTRODUCTION TO APPENDICES

What follows supplements and expands upon material already presented in the text. Because of both its volume and its level of technical detail (i.e., citations to statutes, cases and pending legislation), the appendix format has been adopted for presentation of these additional materials.

There are seven technical appendices to the LRS. They address, respectively, the following topics:

- Appendix "A"--Sample of Traditional State Statutes Used to Prosecute Computer Crimes,
- Appendix "B"--Sample of Federal Laws Used to Prosecute Computer Crime Cases,
- Appendix "C"--Selected Computer Related Crime Evidence Cases,
- Appendix "D"--State Laws Classifying Computer Generated Evidence As Hearsay,
- Appendix "E"--Sample of State Statutes Providing for Confidentiality of Computerizable Information,
- Appendix "F"--Update on Recent State Computer Related Crime Legislation, and
- Appendix "G"--Summary of Federal Computer Systems Protection Act.

It must be emphasized here that while each of these technical appendices is intended to be, and is, extremely comprehensive, it has not been the authors' purpose to render any of them all-inclusive, and no representation to that effect is intended or implied. Indeed, any effort to report on the state of the law nationwide in a particular subject area--whether computer related crime or otherwise--at a particular point in time will necessarily run up against the dynamics of our legal system, where ongoing legislative and court action is constantly making new law. For that reason, any publication which attempts to reflect the state of the law in a given field will, by the time it reaches print, be overtaken by new developments, which inevitably will render it dated in certain of its particulars.

Certainly in the area of computer related crime, where the state of the law is in many respects unsettled and evolving almost daily, this is very much the case. The reader should

therefore be mindful when approaching the materials which follow that they do not represent the definitive compilation of all statutes, regulations and cases of possible applicability to computer related crime because in fact they cannot.

APPENDIX "A"

SAMPLE OF TRADITIONAL STATE STATUTES

USED TO PROSECUTE COMPUTER CRIMES

I. EMBEZZLEMENT - (Covers officers, directors, employees, and others in a fiduciary relationship to the victim):

ALABAMA

14 126
Embezzlement by officer, clerk, agent, servant or apprentice

14 131
Embezzlement of fraudulent secretion by officer, etc., of a corporation

14 132
Embezzlement; banks or broker

ALASKA

11.20.280
Embezzlement by employee or servant

11.20.340
Embezzlement by fiduciary

ARKANSAS

67-706
Banks and other financial institutions; embezzlement and misapplication of funds; officer or employee acting without authority; false entries; penalty

67-707
False entries in books; false papers for deception of commmissioners; false statements concerning affairs of banks; bribery of commissioner

CALIFORNIA

Pen. 504b
Sale of property covered by security agreement; willful failure to notify party; and appropriation of proceeds to own use; punishment

Pen. 506
Person controlling or entrusted with property of another; misappropriated payment of laborers and materialmen as use of contract price

Fin. 3531
International and foreign banking; offenses and penalties

COLORADO

10-12-331
Mutual insurance; false entries; theft; penalties

11-11-107
Financial institutions; embezzlement or misapplication of funds

FLORIDA

661.34
Banks and banking; penalty for embezzlement of funds by conservation

HAWAII

403-143
Bank Act of 1931; embezzlement of funds or assets; penalty

405-32
Trust companies; offenses; penalties

407-34
Savings and loan associations; boards of directors, officers, employees

IDAHO

18-2402
Embezzlement by public and corporate officers

18-2405
Embezzlement by clerk, agent or servant

18-2406
Embezzlement by trustee, banker, agent or fiduciary

18-608
Banks and banking; penalty for officer overdrawing account

26-1104
Banks and banking; embezzlement

ILLINOIS

32 496.39
Corporations; credit unions; embezzlement; sentences

IOWA

710.9
Embezzlement by bank officers or employees

KANSAS

9-2012
Banks; embezzlement; intent to defraud; punishment

KENTUCKY

434.010
Embezzlement by officer, agent or employee of corporation

LOUISIANA

6.324
Fiduciary; security for deposits in capacity of; appropriations of funds; penalty

MARYLAND

27 128
Embezzlement by bank president or director

27.129
Embezzlement by cashier, servant, agent, clerk, etc.; description of items in indictment

MASSACHUSETTS

266 52
Bank officers and employees; fraud or embezzlement

266 53
Bank officers or employees; prosecution for fraud or embezzlement

MICHIGAN

750.174
Embezzlement; agent, servant, employee, trustee, bailee, custodian.

750.362
Larceny; by conversion, etc.

MISSISSIPPI

97-11-25
Embezzlement; officers, trustees and public employees converting property to own use

MISSOURI

369.195
Savings and loan associations; directors and officers to give bond

MONTANA

5-1044
Banks and banking

NEBRASKA

8-110
Banks and banking; banks, executive officers; employees, bonds; felony approval; open to inspection

28-547
Embezzlement and frauds by bank officers; penalty

NEVADA

668.055
Banks and banking; embezzlement; willful misapplication of funds; penalty

NEW HAMPSHIRE

384.20
Savings banks; trust companies, etc.; embezzlement; false entries

NEW JERSEY

2A:102-4
Embezzlement by officers or employees of banks

2A:91-4
Officers of banks overdrawing accounts

NEW MEXICO

3-1-7
Bank account in name of fiduciary; check drawn by fiduciary; balance to principal

33-1-8
Bank account in name of principal; check drawn by fiduciary; balance to principal

NORTH CAROLINA

14-93
Embezzlement by treasurers of charitable and religious organizations

53-129
Banks; misapplication, embezzlement of funds, etc.

53-130
Banks; making false entries in banking acounts; misrepresenting liabilities of banks

NORTH DAKOTA

6-05-16
Banks; indebtedness of directors; prohibition and exception

OHIO

1129.2
Banks; misapplicaiton of funds and false representations

OKLAHOMA

6 1412
Banks and trust companies; embezzlement or misapplication of funds

21-1452
Embezzlement by officer, etc., or corporation, etc.

PENNSYLVANIA

18 4113
Misapplication of entrusted property and property of government institutions

RHODE ISLAND

11-41-11
Embezzlement by bank officer or employee

TENNESSEE

39-4232
Embezzlement by private officer; clerk or employee; penalty

TEXAS

432.413
Banks and banking; officers, employees, agents; embezzlement and misapplication; penalty

852a 11.14
Savings and loan associations; penalty for embezzlement

UTAH

76-10-706
Corporation; unlawful acts by director, officer or agent

VERMONT

13 2532
Officer or servant of incorporated bank

VIRGINIA

6.1-122
Embezzlement, fraud, false statements, etc.; by officer, director, agent, or employee of bank, trust company or trust subsidiary

18.2-113
Fraudulent entries, etc., in accounts by officers or clerks of joint stock companies

WEST VIRGINIA

61-3-22
Falsifying accounts; penalty

WISCONSIN

215.12
Savings and loan associations; penalty for dishonest acts; falsification of records

221.39
State banks; theft; how punished

WYOMING

13-198
Banks; embezzlement; misapplication of funds, etc.; generally certificates of deposit, drafts, etc.; false entries in books, etc.; aiding or abetting violation of section

II. ARSON - (Malicious burnings of a dwelling that housed a computer should be covered):

ALABAMA

14 23-32
Arson

ALASKA

11.20.010-060
Arson, degrees

ARKANSAS

41-1902
Definitions; arson

ARIZONA

13-235
Arson with intent to defraud insurer; punishment

CALIFORNIA

Pen. 448a
Arson: private building other than dwelling

Pen. 449a
Arson: Personal property; punishment

Pen. 450a
Arson: personal property with intent to defraud insurers; punishment

COLORADO

18-4-101-105
Arson

CONNECTICUT

53a-112
Arson in the second degree; class C felony

DELAWARE

11 801-811
Arson and related offenses

FLORIDA

817.233
Burning to defraud insurer

GEORGIA

26-14
Arson and related offenses

HAWAII

Chapter 723
Arson

723-10
Willful burning with intent to defraud insurers; penalty

IDAHO

18-801-804
Arson

ILLINOIS

38 21-1
Criminal damage to property

INDIANA

35-16-1-1
Arson in the first degree (in defrauding insurer)

IOWA

707.4
Defrauding insurers (arson)

KANSAS

21-3718
Arson

KENTUCKY

433.010
Arson

433.040
Burning personal property to defraud insurer

LOUISIANA

14.53
Arson with intent to defraud

MAINE

17-A 801-806
Arson and other property destruction

MARYLAND

27 6-11
Arson

27 9
Arson: burning goods, wares, etc., with intent to defraud insurer

MASSACHUSETTS

266 10
Insured property, burning with intent to defraud

MICHIGAN

750.75
Burning of insured property

MISSISSIPPI

15-3-9
Prevention of frauds; creditors to be notified of destruction of insured stock of merchandise by fire

97-17-11
Arson; insured property

MISSOURI

560.030
Arson of insured property

MONTANA

94-6-103
Negligent arson

NEBRASKA

28-504.05
Arson; burning to defraud insurer; penalty

NEVADA

205.030
Arson; burning or aiding and abetting burning of property with intent to defraud insurer; penalty

NEW HAMPSHIRE

634.1
Arson

NEW JERSEY

2A:89-3
Arson; setting fire to or burning property to defraud

NEW MEXICO

40A-17-5
Arson or negligent arson

NEW YORK

Penal 150.00-20
Arson

NORTH CAROLINA

12.1-21-01
Arson

OHIO

2090.01.11
Arson

2913.01
Theft definition

OKLAHOMA

21 1201-1403
Arson

OREGON

164.305-325
Arson

RHODE ISLAND

11-4-5
Arson; burning with intent to defraud insurer

SOUTH CAROLINA

16-311-313
Arson; burning to defraud

SOUTH DAKOTA

22.23-4
Arson; burning to defraud insurer as felony

TENNESSEE

39-506
Arson; burning of insured property

TEXAS

Penal Code 28.02
Arson

UTAH
76-6-102
Arson

VERMONT

13 506
Arson; burning to defraud insurer

VIRGINIA

18.2-77 to 81
Arson

WASHINGTON

9A.28.010-030
Arson

WEST VIRGINIA

61-3-5
Arson; burning or attempting to burn, insured property

WISCONSIN

943.02 to 04
Arson

WYOMING

6-125
Arson to defraud insurer

III. BANK RELATED FRAUDS - (using the computer of a financial institution for purposes of a fraud could be covered by the following):

ALASKA

06.05.505
Banks and financial institutions; unlawful to transmit reports required by department

06.05.510
Banks and financial institutions; unlawful false report to department

ARKANSAS

41-2306
Issuing a false financial statement

67-708
Officers, agent or clerk making false reports or false entries in books (bank); exhibition of false papers with intent to deceive; penalty

ARIZONA

6-392
False or deceptive entries or statements of a bank; penalty

6-485
False statements as to financial condition of savings and loan associations

CALIFORNIA

Pen. 532a
False financial statements; punishment

Pen. 484c
Submission of false voucher to obtain construction loan funds

Fin. 3351
Overdrafts by bank officers and employees

Fin. 3361
Misapplication of bank assets

CONNECTICUT

36-6
Banking; false statements, entries or reports; penalty

DELAWARE

5 123
Banking; false statements, entries or reports; penalty

FLORIDA

817.16
False reports, etc. by officers of banks, trust companies, etc., under supervision of Department of Banking and Finance with intent to defraud

HAWAII

403-147
Banks and financial institutions; fraudulent insolvency; penalty

407-34
Savings and loan associations; boards of directors, officers and employees

ILLINOIS

32-848
Savings and Loan Act: commissioners

INDIANA

28-1-20-6
Banks; borrower misrepresenting age or other facts to bank or trust

IOWA

524.1607
Banks; false statement for credit

KANSAS

9-2001
Banks--codes; crimes and punishments

KENTUCKY

517.110
Business and commercial frauds; misapplication of entrusted property

LOUISIANA

6:931
Banks and banking: false statements and similar actions prohibited

MAINE

9B 466
Financial institutions: unlawful acts

MARYLAND

11 75
Banks and trust companies; false statements or entries, accepting deposits knowing institution to be insolvent

27 148
False statement of financial condition or ability to pay

MASSACHUSETTS

167 5
Commissioner of banks; power to report and prosecute violations of loan review

266 53
Bank officers and employees: misconduct; penalty

MICHIGAN

750.101
Bank, deposit and trust companies; financial institutions

MISSISSIPPI

81-5-1
Banks and banking; general regulations

MISSOURI

561.500
Bank officer concealing loans; misdemeanor

MONTANA

5-1041
Banking: concealment of loans and discounts

NEBRASKA

8-110
Banks and banking; banks; executive officers; employees' bonds; felony; approval; open to inspection

8-225
Trust companies; false statement or book entry; destruction or secretion of records; penalty

NEW HAMPSHIRE

384.17
Savings banks; trust companies; false statements

384.20
Savings banks; trust companies; embezzlement; false entries

NEW JERSEY

2A:19-3
Banks and financial corporations; false reports as to solvency of bank

2A:91-5
Banks and financial corporations; false entries by bank officers

2A:91-7
Banks and financial corporations; building and loan and other associations; false statements, entries or reports to deceive examiners

2A:91-8
Banks and financial corporations; building and loan and other associations; director or officer: false statement or report or misrepresentation

NEW YORK

Bank 660
Misconduct or officers; directors; trustees or employees of banking corporations and of private bankers

Bank 663
Receiving deposits in insolvent bank

Bank 664
Unlawful investments by officers of savings banks

Bank 672
Falsification of books, reports or statements by private bankers or corporations subject to the banking law

NORTH CAROLINA

53-129
Banks; misapplication, embezzlement of funds, etc.

NORTH DAKOTA

6-08-14
Banks, false statements concerning bank values; penalty

OHIO

1129.02
Banks; misapplication of funds and false representation

1129.05
Banks; false representations

19-19-8
Examination of books to determine violations; prosecution of offenses

SOUTH CAROLINA

8-108
Banking; false statements concerning solvency of bank

TENNESSEE

1153.99
Building and loan associations; penalties

11701.96
Corporations; preparation of false reports

OKLAHOMA

6 1414
Banking; criminal sanctions; violation of rules and orders: nonapplicable where criminal sanctions imposed in other sections of code

OREGON

706.725
Banks and trust companies; false statement; reports and book entries

PENNSYLVANIA

18 4112
Receiving deposits in a failing financial institution

RHODE ISLAND

11-18-8
False representation as to continuing trust of financial statements

TEXAS

342.413
Banks and banking; officers, employees, agents; embezzlement, abstraction and misapplication; penalty

UTAH

76-6-512
Acceptance of deposit by insolvent financial institution

VIRGINIA

6.1-195.73
Savings and loans; false statements by officers or agents

WASHINGTON

33.36.040
Savings and loan associations; falsification of books, etc.

33.36.050
Savings and loan associations; false statement affecting financial status

33.36.060
Savings and loan associations; suppressing, secreting or destroying records

WEST VIRGINIA

31A-8-8
Banks and banking; false statements concerning banking institutions

31A-8-9
Banks and banking; misapplication of funds, fraud by officers or employees; false entries in books, false statements; penalties

WISCONSIN

215.12
Savings and loan associations; penalty for dishonest acts; falsification of records

221.39
State banks; theft; how punished

IV. BUSINESS RELATED FRAUDS

ALABAMA

14 219
Keeping false books or accounts by officers or agents of corporation

ALASKA

11.20.430
Falsifying or destroying corporate or company records

ARKANSAS

41-2302
Falsifying business records

ARIZONA

13-318
Fraud on business establishment; punishment; prima facie evidence of intention to defraud

44-1212
False report to principal by agent; penalty

CALIFORNIA

Corp. 2200-2260
Crimes and penalties; include false signatures, false statements, fraud by directors, unlawful possession of corporation property, foreign corporation

Civil Code 2306
Defrauding principal, agent without authority

Pen. 154
Debtor fraudulently removing, conveying or concealing property, punishment

COLORADO

18-5-201
Fraud in obtaining property or services; definitions

18-5-206
Defrauding a secured creditor or debtor

DELAWARE

11 281
Criminal liability of corporation

11 871
Falsifying business records

FLORIDA

817.15
Making false entries, etc., on books of corporations

IDAHO

18-1905
Corporations; falsification of corporate books

18-1906
Corporations; fraudulent reports by officers

18-1908
Corporations; director deemed to have knowledge of affairs

ILLINOIS

59 1
Frauds and perjuries; writing necessity; signature

59 3
Frauds and perjuries; considered proof

59 5
Frauds and perjuries; innocent purchaser

IOWA

491.40
Corporations; penalty for fraud

491.43
Corporations; keeping false accounts

41.68
Corporations; false statements, pretenses

713.26
False entries in corporation books

KENTUCKY

439.090
Misrepresentations as to financial condition

434.110
Alteration or destruction of company records by officer or employee

517.050
Business and commercial frauds; falsifying business records

MASSACHUSETTS

1818 10
Foreign corporations; false reports or statements; signing by directors and officers: liability to creditors; report of condition exceptions

266 67
Corporate books; false entries; intent to defraud

MICHIGAN

450.49
Corporations; false reports, certificates and other statements; penalties

450.1932
Corporations; false or fraudulent statements and false or wrongfully altered records; penalties

450.1935
Corporations; liability for false material representation or wrongful alteration of statement, records, or public notices; limitation of actions

NEVADA

205.405
Falsifying accounts

NEW JERSEY

2A:11-9
Destruction or alteration of false entries in books or papers of corporation, partnership or association

2A-111-10
Keeping fraudulent accounts by directors, officers, etc. of corporation, partnership or association

NEW YORK

Penal 175.00-15
Falsifying business records

OHIO

1701.93
Corporations; false statement or entry

1701.94
Corporations; forfeiture for failure to maintain or furnish certain records

2913.42
Tampering with records

OKLAHOMA

21 1634
Corporation affairs; omitting to enter receipt

21 1635
Corporation affairs; destroying or falsifying books

21 1636
Corporation affairs; false reports of corporation

18 3926
Theft of services

18 4103
Fraudulent destruction, removal or concealment of recordable instrument

184104
Tampering with records or identification

OREGON

164.125
Theft of services

165.080
Falsifying business records

165.100
Issuing a false financial statement

SOUTH DAKOTA

47-30-3
Corporate frauds and mismanagement; fraudulent prospectus or report; felony; punishment

47-30-4
Corporate frauds and mismanagement; fraudulent entries in corporate books; misdemeanor

47-30-6
Corporate frauds and mismanagement; fraudulent mutilation or falsification of corporate books; punishment

TENNESSEE

39-1905
False entries on books; penalty

TEXAS

Penal Code 31.04
Theft of service

Penal Code 32.32
False statement to obtain property or credit

UTAH

76-6-503
Fraudulent handling of recordable writings

76-6-504
Tampering with records

VERMONT

13 2582
Theft of services

VIRGINIA

18.2-186
False statements to obtain property or credit

WASHINGTON

9.24.050
Corporations: false report of corporation

WEST VIRGINIA

19-4-26
False reports about finances or management of cooperative associations; penalty

61-3-37
False statement as to financial condition of person, firm or corporation; penalty

WISCONSIN

180.88
Corporations; penalty for false statements

185.82
Cooperatives; filing and recording documents; penalty for false document

943.39
Fraudulent writings

943.40
Fraudulent destruction of certain writings

WYOMING

18-289-22
False statement or misrepresentation; penalty; subdivisions for sale

V. FORGERY

ALABAMA

14-199-208
Forgery

ALASKA

11.25-010-11.25.130
Forgery and counterfeiting

ARKANSAS

41-2302
Forgery

41-2812
Criminal possession of forgery device

CALIFORNIA

Pen. 470-473
Forgery and counterfeiting

COLORADO

18-5-101-109
Forgery

CONNECTICUT

53a-137
Forgery

DELAWARE

11 861-63
Forgery and related offenses

FLORIDA

831.04
Penalty for changing or forging certain instruments of writing

GEORGIA

26-1701-1703
Forgery

HAWAII

Chapter 743
Forgery

IDAHO

18-3600-20
Forgery

INDIANA

35-1-124-1
Forgery

IOWA

713.1
False pretenses (includes forgery)

KANSAS

21-3710-3714
Forgery (includes making false writing, destroying written instrument, altering legislative document, possession of forgery devices)

KENTUCKY

516.010-110
Forgery

LOUISIANA

14:72
Forgery

MAINE

17-A 701-708
Forgery and related offenses (includes criminal simulation, falsifying private records, suppressing recordable instrument)

MARYLAND

27-44
Forgery

27 612
Indictment for forging, altering, embezzling, etc., an instrument; intent to defraud; description of instrument

MASSACHUSETTS

267 1
Forgery

MICHIGAN

750-248
Forgery

MINNESOTA

609.63.625
Forgery

MISSISSIPPI

97-21-1 to 63
Forgery and counterfeiting

MISSOURI

561.011
Forgery

MONTANA

94-6-310
Forgery

NEBRASKA

28-601
Forgery

NEVADA

205.085 to 217
Forgery

NEW HAMPSHIRE

638.1
Forgery

NEW JERSEY

2A:109-1
Forgery

2A:159-3
Forgery, larceny or embezzlement or conspiracy to commit same, conspiracy to defraud by public officers, fiduciaries, etc.

NEW MEXICO

40A16-9
Forgery

NEW YORK

Penal 170.00
Forgery

NORTH CAROLINA

14-119 to 125
Forgery

NORTH DAKOTA

12.124-01 to 05
Forgery

OHIO

2913.31
Forgery

OKLAHOMA

21 1561-1627
Forgery

OREGON

165.002-013
Forgery

PENNSYLVANIA

18 4101
Forgery

RHODE ISLAND

11-17-1
Forgery and counterfeiting in general

SOUTH CAROLINA

16-351
Forgery

SOUTH DAKOTA

22-39-36 to 39
Forgery

TENNESSEE

39-1701 to 1712
Forgery

TEXAS

CCP 38.19
Intent to defraud in forgery

Penal Code 32.21
Forgery

UTAH

76-6-501, 502
Forgery

VERMONT

13 1801-1806
Forgery

VIRGINIA

18.2-169 to 173
Forgery

WASHINGTON

9A.60.020
Fraud, forgery

WEST VIRGINIA

61-4-5
Forgery

WISCONSIN

943.38
Forgery

WYOMING

6-17 to 21
Forgery

APPENDIX "B"

SAMPLE OF FEDERAL LAWS

USED TO PROSECUTE COMPUTER CRIME CASES

18 U.S.C. 641: Proscribes embezzlement or theft of public money, property or records. This statute covers only Federal money, property and records; however, its authority extends to both the thief and the receiver of the property.

18 U.S.C. 659: Proscribes theft of goods or chattel moving as, which are part of, or which constitute interstate commerce; goods must be in interstate commerce at time of theft.

18 U.S.C. 661: Proscribes theft within a special maritime or territorial jurisdiction; and theft within a Federal enclave.

18 U.S.C. 81: Makes it unlawful to commit arson within a Federal enclave. Courts, however, have interpreted statutory language narrowly here. See U.S. v. Banks, 368 F Supp 1245 (1973).

18 U.S.C. 793: Makes unlawful the gathering, transmitting, or losing of defense information; statute reaches property owned, used, leased, etc., by Federal government contractors when related to national defense. Has potential applicability where abuse involves classified, restricted or national defense computer software.

18 U.S.C. 794: Proscribes gathering, transmitting, or delivering of national defense information to foreign government, agent or power. Classification of information is immaterial; it is necessary to demonstrate that disclosure leads to "substantial injury" to national defense. See New York Times Co. v. U.S., 403 U.S. 713 (1971).

18 U.S.C. 795: Prohibits photographing and sketching of defense installations. Mere copying of certain types of classified computer software could be prosecuted under this statute.

18 U.S.C. 797: Proscribes publication and sale of photographs or sketches of equipment of military and defense installations.

18 U.S.C. 799: Establishes standards for security violations of National Aeronautics and Space Administration (NASA) regulations.

18 U.S.C. 912: Makes it unlawful to obtain a thing of value by impersonating an officer or employee of the Federal government.

18 U.S.C. 952: Prohibits the intentional disclosure of diplomatic codes.

18 U.S.C. 371: Defines conspiracy; makes it unlawful for two or more persons to conspire to defraud the Federal government.

18 U.S.C. 471-509: Forgery and counterfeiting statutes; limited applicability in current statutory form.

18 U.S.C. 656, 657: Makes theft, embezzlement, and the like unlawful where the perpetrator is an employee, officer, agent or is connected with a Federally regulated bank or savings and loan association.

18 U.S.C. 1005, 1006: Proscribes the making of false entries in bank and credit institution records, including omissions, obliterations, alterations.

18 U.S.C. 1341, 1342: Makes it unlawful to use the mails for the purpose of executing or attempting to defraud or scheme to obtain money or property under false pretenses.

18 U.S.C. 1343: Proscribes the use of wire communications to execute or attempt to execute a fraud or scheme to obtain money or property under false pretenses; message must cross State lines.

18 U.S.C. 1361: Proscribes malicious injury to Federal property.

18 U.S.C. 1905: Prohibits disclosure of confidential information; however, applies only to Government officials, employees, and Federal contractors.

18 U.S.C. 2071: Makes unlawful the concealment, mutilation or removal of public records.

18 U.S.C. 2113: Proscribes burglary of a bank; however, must show forcible entry.

18 U.S.C. 2115: Proscribes burglary of a post office; but must show forcible entry.

18 U.S.C. 2117: Proscribes burglary of an interstate carrier facility; but must show forcible entry.

18 U.S.C. 2152: Proscribes trespassing on fortifications or harbor-defense areas.

18 U.S.C. 2153: Provides penalties for destruction of property affecting national security.

18 U.S.C. 2314: Proscribes the interstate transportation of stolen property; property must cross State lines, not merely be introduced into interstate commerce. Copies of valuable geophysical maps taken into interstate commerce were found to be theft of "valuable idea". See U.S. v. Lester, 282 F.2d 750 (1960). Copies of computer programs could come under this statute.

18 U.S.C. 2511, 2516, 2517, 2518, and 520, (Title III, Omnibus Crime Control Act of 1968: Makes it a crime to willfully intercept any wire or oral communications; relates to privacy of the individual; must be understandable to human ear.

APPENDIX "C"

SELECTED COMPUTER RELATED

CRIME EVIDENCE CASES

Transport Indemnity Co. v. Seib, 178 Neb. 253, 132 N.W.2d 871 (1965)--State court reasoned that a computer printout consisted of data retrieved for trial purposes and was not specifically prepared for trial; it allowed in as evidence under the Uniform Business Records as Evidence Act the proponent's computer-prepared exhibit on the ground that the data were computerized in the regular course of business.

Merrick v. US Rubber Co., 440 P.2d 314 (1968)--State court of appeals allowed in evidence computer printouts supporting plaintiff's claim of money owed by defendant, despite fact that plaintiff's witness testified that he had no personal knowledge of the physical operation of the plaintiff's computer system; court observed that the defendant did not challenge the substance of the records or their accuracy, and acknowledged the occurrence of the transactions. (See also State v. Veres, 436 P.2d 629 (1968).)

King v. State ex rel. Murdoch Acceptance Corp., 222 So.2d 393 (1969)--State court, applying the common law shop-book rule, allowed in evidence computer printouts that purportedly reflected the balance due on six conditional-sales contracts. Defendant argued that the printouts were not original documents and did not fall within the rule, but the court cited Seib, supra, and ruled that society's needs and the needs of the new business era indicated that a liberal interpretation of the common-law rule was necessary.

Olympic Insurance Co. v. Harrison, Inc., 418 F.2d 669 (1969)--Fifth Circuit Court of Appeals admitted in evidence IBM computer printouts to establish that the defendant owed the plaintiff over $300,000 in insurance premiums on policies written by the defendant as the plaintiff's agent. Court rejected the defendants's claim that the printouts were unreliable, and the defendant failed to raise objections as to the accuracy and reliability of the computerization of the records.

United States v. De Georgia, 420 F.2d 889 (1969)--Ninth Circuit Court of Appeals admitted evidence under the Federal Business Records Act consisting of computer records which showed that an automobile allegedly stolen by the defendant in fact was owned by Hertz Rental Company, was missing and had not been rented out; a Hertz employee familiar with the company's computer system

testified that he received information that the car had been stolen and used the master control to ascertain that the auto was missing. The court ruled that regularly maintained business records are admissible as an exception to the hearsay rule.

Arnold D. Kamen & Co. v. Young, 466 S.W.3d 381 (Tex. Civ. App. 1971)--Texas Courts of Appeals affirmed a lower court ruling that computer printouts of certain financial statements were inadmissible because the proponent's witness who testified concerning the printouts did not have personal knowledge concerning the information on the printouts and merely testified that the information was prepared by an employee of the proponent. (See also People v. Gauer, 288 N.E.2d 24 (1974).)

City of Seattle v. Heath, 520 P.2d 1392 (Wash. State 1974)--State court of appeals upheld lower court's ruling admitting State's Department of Motor Vehicles' computer records concerning the defendant's driving record and the status of his drivers' license. Interpreting the State's business records statute broadly, the court held that a record that has been computerized and stored in a computer's data bank is admissible, like any other form of record; since the computerization of the written documents was done in the regular course of business and since there was a strong public policy consideration involved in such license-type records, the court looked favorably on the prosecution's efforts to introduce DMV computer records.

United States v. Dioguardi, 428 F.2d 1033 (2nd Cir. 1970), cert. denied, 400 U.S. 825--Second Circuit Court of Appeals affirmed a lower court's conviction for the defendants' fraudulent transferring and concealing of the property of a bankrupt in contemplation of bankruptcy. The appeals court, noting that the Government prosecutors employed a computer to trace the bankruptcy fraud in order to recreate what happened, acknowledged that the defendants had a right to know what the computer was programmed to do and had a right to use the computer program on cross-examination if they so desired. However, because there was no appreciable risk that prejudice occurred, the computer operations involved were relatively simple and could have been checked with an adding machine or manually, failure to compel production of the programs did not warrant a new trial, the court concluded.

United States v. Russo, 480 F.2d 1228 (6th Cir. 1973), cert. denied, 414 U.S. 1157--Sixth Circuit Court of Appeals overruled several objections to the admission of computer printouts indicating that the defendants had filed false pay vouchers with a medical insurance carrier for services never rendered. The court of appeals affirmed the lower court's finding that the computer

records were trustworthy, even though prepared at a date later than that which the event occurred; that a proper foundation had been laid; and that the defense in fact had adequate time to make tests and examine the computerized evidence.

United States v. Greenlee, 517 F.2d 890 (3rd Cir. 1975)--Third Circuit Court of Appeals admitted in evidence manually and computer-prepared records stored in the Internal Revenue Service's computer system, to be used in the prosecution of an attorney for willful failure to file an income tax return; the appeals court was apparently aware of the ramifications which an adverse ruling would have had in the enforcement of the Internal Revenue Code, since most such records are computerized. This public policy consideration, like DMV-computer records in Heath, supra, weighed heavily in the court's decision.

United States v. Liebert, 519 F.2d 542 (3rd Cir. 1975)--Third Circuit vacated judgement of lower court ordering Federal prosecutors involved in prosecuting individual for willful failure to file income tax returns to furnish the defendant with a portion of the lists of nonfilers for the years in question; the appeals court conceded that the defendant had a right to gain access to the IRS computers, to allow his experts to study all IRS procedures, but it also acknowledged that full disclosure as the defendant requested could involve the privacy rights of many third parties. The appeals court recommended that the government produce material and experts necessary to conduct an adequate test of the IRS computer system, but it allocated the costs so that each party would pay only that for which it was responsible. This result arguably limits a party's case to the best evidence which it can afford to present.

Harned v. Credit Bureau, 513 P.2d 650 (Wyo. 1973)--The court barred a computer-generated summary of accounts because it violated the Best Evidence Rule.

APPENDIX "D"

STATE LAWS

CLASSIFYING COMPUTER GENERATED EVIDENCE

AS HEARSAY

STATE	STATE LAW CITATION
ALABAMA	Code of Ala., Tit. 7, §§ 415(1), 415(2).
ALASKA	A.S. Rules of Civ., Proc., Rule 44(c).
ARKANSAS	Ark. Stats. § 28-932.
CALIFORNIA	West's Ann. Evidence Code §§ 1550, 1551.
COLORADO	C.R.S. '73, 13-26-101 to 13-26-104.
CONNECTICUT	C.S.G.A. § 52-180.
DELAWARE	10 Del.C. § 4309.
GEORGIA	Code § 38-710.
HAWAII	HRS § 622-4.
IDAHO	I.C. §§ 9-417 to 9-419.
1OWA	I.C.A. § 622.30.
KANSAS	K.S.A. 60-469.
KENTUCKY	KRS 422.105.
MAINE	16 M.R.S.A. § 456.
MARYLAND	Code, Courts and Judicial Proceedings, "§ 10-102."
MASSACHUSETTS	M.G.L.A. c 233, § 79E.
MICHIGAN	M.C.L.A. § 600.2147.
MINNESOTA	M.S.A. § 600.135.
MONTANA	R.C.M. 1947, § 93-801-5, 93-801-6.
NEBRASKA	R.R.S. 1943, §§ 25-12,-112 to 25-114.
NEW HAMPSHIRE	RSA 520:1 to 520:3.
NEW JERSEY	N.J.S.A. 24:82-38 to 2A: 32-40.
NEW MEXICO	1953 Comp. §§ 20-2-20 to 20-2-22.
NEW YORK	McKinney's CPLR 4539.
NORTH CAROLINA	G.S. §§ 8-45.1 to 8-45-4.
NORTH DAKOTA	NDCC 31-08-01.1.
OKLAHOMA	12 Okl. St. Ann. §521 to 523.
PENNSYLVANIA	28 P.S. §§ 141 to 143.
RHODE ISLAND	Gen. Laws 1956, § 9-19-14.
SOUTH DAKOTA	SDCL 19-7-12.
TENNESSEE	T.C.A. § 24-711.
UTAH	U.C.A. 1953, 78-25-16.
VERMONT	12 V.S.A. § 1701.
VIRGIN ISLANDS	5 V.I.C. § 956.
VIRGINIA	Code 1950, §§ 8-279.1, 8279.2.
WASHINGTON	RCWA 5.46.010 to 5.46.920.
WEST VIRGINIA	Code, 57-1-7b.
WISCONSIN	W.S.A.889.29.
WYOMING	W.S. 1957, §§ 1-174 to 1-177.

APPENDIX "E"

SAMPLE OF STATE STATUTES

PROVIDING FOR CONFIDENTIALITY OF COMPUTERIZABLE INFORMATION

A. Medical Records

Alaska

1. "Disclosure of Information", Alaska Stat. sec. 47.30.260

Connecticut

1. "Procedure Where Right To Inspect Records Is Denied", Conn. Gen. Stat. Ann. sec. 4-105*
2. "Mental Health Information--The Transfer and Storage Of", Conn. Gen. State. Ann. sec. 52-146h
3. "Availability of Patient Information to Certain Agencies", Conn. Gen. Stat. Ann. sec. 17-295c*

Delaware

1. "Report of V.D. Cases", Del. Code Ann. tit. 16, sec. 702
2. "Child Under Treatment By Spiritual Means Not Neglected", Del. Code Ann. tit. 16, sec. 907

Georgia

1. "Conditions for Disclosure of Confidential Information", Ga. Code Ann. sec. 38-717.21
2. "Employment Outside the Facility", Ga. Code Ann. sec. 88-502.10

Hawaii

1. "Medical Records", Hawaii Rev. Stat. sec. 622-51

Key: *Cases Reported

2. "Sources of Information Protected", Hawaii Rev. Stat. sec. 324-11

3. "Identification of Persons Studied; Restricted", Hawaii Rev. Stat. sec. 324-12

Idaho

1. "Confidential Relations and Communications", Idaho Code sec. 9-203(4)*

2. "Licensure By Written Examination", Idaho Code sec. 54-1810(h)(2)

3. "Proof of Medical Charts or Records by Certified Copy", Idaho Code sec. 9-420

Iowa

1. "Communications in Professional Confidence", Iowa Code Ann. sec. 622.10*

2. "Public Health", Iowa Code Ann. sec. 140.1-4

Kansas

1. "Disclosure of Records", Kan. Stat. Ann. sec. 59-2931

Maryland

1. "Confidential Records", Md. Ann. Code art. 43, sec. 1-I

2. "Report of Laboratory Indicating V.D. or T.B.", Md. Ann. Code art. 43, sec. 31A

3. "Medical Files Available for Inspection By Claimant", Md. Ann. Code art. 48, sec. 490C

Minnesota

1. "Physicians and Surgeons", Minn. Stat. Ann. sec. 595.02(4)*

Oklahoma

1. "V.D. Cases--Instructions--Notification", Okla. Stat. tit. 63, sec. 1-528(b)*

2. "Health Services for Minors", Okla. Stat. tit. 63, sec. 2601*

3. "Access to Medical Records", Okla. Stat. tit. 76, sec. 19

Tennessee

1. "Access to Medical Records", Tenn. Code Ann. sec. 53-1322

Texas

1. "Providing Data to the State Department of Health", Tex. Stat. Ann. art. 4447D*

Vermont

1. "Treatments, Refusals, Penalty", Vt. Stat. Ann. tit. 18, sec. 1092

2. "Examination and Report", Vt. Stat. Ann. tit. 18, sec. 1093

3. "Reports and Records Confidential", Vt. Stat. Ann. tit. 18, sec. 1099

Virginia

1. "Procedure for Requesting Records for Inspection", Va. Code sec. 2.1-342(b)

2. "Copies of Hospital Records and Patient Records", Va. Code sec. 8-277.1

B. Financial Records

Alaska

1. "Books and Records to be Kept Confidential", Alaska Stat. sec. 6.30.120

2. "Depositor and Customer Records Confidential", Alaska Stat. sec. 6.05.175

2. "Consumer Credit Reporting Agencies Act", Cal. Civ. Code sec. 1785

3. "Giving of False or Unfavorable Credit Information", Cal. Civ. Code sec. 1747.70

4. "Disclosure of Information Concerning Private Trust", Cal. Fin. Code sec. 1582

5. "Policy Information Available to Solicitors: Restrictions", Cal. Ins. Code sec. 770.1

Connecticut

1. "Truth and Lending Act", Conn. Gen. Stat. 36-393*

Iowa

1. "Confidentiality", Iowa Code Ann. sec. 527.10

Kansas

1. "Penalties", Kan. Stat. Ann. sec. 50-720

Kentucky

1. "Inspection of Books--Records Confidential", Ky. Rev. Stat. Ann. sec. 289.271

Maryland

1. "Disclosure of Finanical Records Prohibited; Exceptions", Md. Ann. Code art. 11, sec. 225

2. "Consumer Credit Reporting Agencies", Md. Com. Law Code Ann. sec. 14-1201

3. "Notice of Service of Subpoena on Issuer to Credit Card Holder", Md. Com. Law Code Ann. sec. 13-312

Massachusetts

1. "Consumer Credit Reporting", Mass. Gen. Laws Ann. ch. 93, sec. 51 thru 58

Minnesota

1. "Access to Books and Records; Communication with Members", Minn. Stat. Ann. sec. 51A.11

Missouri

1. Procedures and Conditions for Inspection of Records", Mo. Ann. Stat. sec. 369.099

Nevada

1. "Prohibited Practices by Collection Agencies", Nev. Rev. Stat. sec. 649.375(7)

New Jersey

1. "Prohibition of Communication on Claimed Billing Error", N.J. Rev. Stat. sec. 56:11-3(c)

New Mexico

1. "Credit Bureaus", N.M. Stat. Ann. sec. 50-18-1

2. "Unauthorized Practices by Licensees or Employees" N.M. Stat. Ann. sec. 67-15-78(B)

New York

1. "Fair Credit Reporting Act", N.Y. Gen. Bus. Law sec. 380

2. "Prohibited Practices", N.Y. Gen. Bus. Law sec. 601.3*

3. "Creditor Billing Errors", N.Y. Gen. Bus. Law sec. 701 thru 707

Oklahoma

1. "Disclosure of Communications and Writing Prohibited", Okla. Stat. Ann. tit. 6, sec. 1013

Oregon

1. "Loan Associations", Or. Rev. Stat. sec. 722.303

Utah

1. "Credit Rating Report Limitations", Utah Code Ann. sec. 70B-10-102

West Virginia

1. "Unreasonable Publication", W. Va. Code sec. 46A-2-126

Wisconsin

1. "Office of Commissioner of Savings and Loan", Wis. Stat. Ann. sec. 215.02

C. Tax Records

Alaska

1. "Disposition of Tax Information", Alaska Stat. sec. 9.25.100

Arizona

1. "Publicity of Returns", Ariz. Rev. Stat. Ann. sec. 43.145

Colorado

1. "Reports and Returns", Colo. Rev. Stat. sec. 39-21-113

Delaware

1. "Secrecy of Returns and Information; Penalty", Del. Code Ann. tit. 30, sec. 1241

Georgia

1. "Secrecy: Reporting to Federal Officers; Preservation of Returns", Ga. Code Ann. sec. 92-3216

Hawaii

1. "Disclosure by Return Preparers", Hawaii Rev. Stat. sec. 231.15.5

Kansas

1. "Secrecy Required; Penalty for Violation; Exceptions", Kan. Stat. Ann. sec. 79-3234

Kentucky

1. "Secrecy of Acquired Information; Exceptions", Ky. Rev. Stat. Ann. sec. 131.190*

Louisiana

1. "Confidential Character of Collector's Records", La. Rev. Stat. Ann. sec. 47:1508

Maine

1. "Powers of Assessor", Me. Rev. Stat. Ann. tit. 36, sec. 5340

Maryland

1. "Secrecy of Returns", Md. Ann. Code art. 81, sec. 300*

2. "Administration", Md. Ann. Code art. 81, sec. 304*

Minnesota

1. "Disclosure of Contents of Tax Returns; Exceptions; Penalty", Minn. Stat. Ann. sec. 290-611

Nebraska

1. "Income Tax; Commissioner, Enforcement of Act", Neb. Rev. Stat. sec. 77-27, 119

New York

1. "General Powers of Tax Commission", N.Y. Tax Law sec. 697*

North Carolina

1. "Secrecy Required by Officials; Penalty for Violation", N.C. Gen. Stat. sec. 105-259

North Dakota

1. "Secrecy as to Returns", N.D. Cent. Code sec. 57-38-57*

Ohio

1. "Additional Powers of the Commissioner", Ohio Rev. Code Ann. sec. 5747.18*

Oklahoma

1. "Records and files of Commission Confidential and Privileged", Okla. Stat. Ann. tit. 68, sec. 205

Oregon

1. "Divulging Particulars of Returns and Reports Prohibited", Or. Rev. Stat. sec. 314.835

Rhode Island

1. "General Powers of Tax Administrator--Secrecy Requirement", R.I. Gen. Laws sec. 44-30-95(c)

Utah

1. "Divulging Information; Exchange of Information with U.S. I.R.S.", Utah Code Ann. sec. 59-14-72

Vermont

1. "Consent to Use or Disclose Information", Vt. Stat. Ann tit. 32, sec. 5901

Virginia

1. "Secrecy of Information", Va. Code sec. 58-46

Wisconsin

1. "Divulging Information", Wis. Stat. Ann. sec. 71.11(44)*

D. Criminal Justice Records

Alaska

1. "Regulations", Alaska Stat. sec. 12.62.010

Arkansas

1. "Creation of Criminal Justice Information Center", Ark. Stat. Ann. sec. 5-1101

2. "Invasion of Privacy", Ark. Stat. Ann. sec. 5-1108

California

1. "Prohibition of Disclosure of Certain Arrest Records", Cal. Lab. Code sec. 437.7*

2. "Prohibition of Disclosure of Certain Arrest Records", Cal. Bus. & Prof. Code sec. 461

3. "Legislative Declaration", Cal. Ins. Code sec. 11580.08

4. "Information Furnished; Application", Cal. Penal Code sec. 11105*

Illinois

1. "Daily Copies of Fingerprints--Duty of Sheriffs and Officers", Ill. Ann. Stat. ch. 38, sec. 206-5*

2. "Records Not to be Made Public", Ill. Ann. Stat. ch. 38, sec. 206-7

Indiana

1. "Criminal Intelligence Information", Ind. Code Ann. 5-2-4

Louisiana

1. "Duty of Peace Officers to Report to District Attorney", La. Rev. Stat. Ann. sec. 15:575

Maryland

1. "Criminal Justice Information System", Md. Ann. Code art. 27, sec. 742

Massachusetts

1. "Criminal Offender Record Information System", Mass. Gen. Laws Ann. ch. 6, sec. 167 thru 178*

Minnesota

1. "Internal Dissemination Prohibited", Minn. Stat. Ann. sec. 15.1643

New Hampshire

1. "Records", N.H. Rev. Stat. Ann. sec. 648.9

New Mexico

1. "Automated Data Processing", N.M. Stat. Ann. sec. 4-25-1

Oklahoma

1. "Law Enforcement Telecommunications System Division--Creation", Okla. Stat. Ann. tit. 47, 2-124

2. "Protection of Information", Okla. Stat. Ann. tit. 47, sec. 2-129

Utah

1. "Access to--Secrecy of", Utah Code Ann. sec. 77-59-27

Washington

1. "Availability of Information", Wash. Rev. Code Ann. sec. 43.43.710

2. "Obtaining Information by False Pretenses--Unauthorized Use of Information--Falsifying Records--Penalty", Wash. Rev. Code Ann. sec. 43.43.810

E. Privacy Acts

Arkansas

1. "Arkansas Information Practices Board", Ark. Stat. Ann. sec. 16-804

California

1. "Title 1.8 Personal Data", Cal. Civ. Code sec. 1798

Connecticut

1. "Personal Data", Conn. Gen. Stat. Ann. sec. 4-190

Indiana

1. "Fair Information Practices", Ind. Code Ann. sec. 4-1-6-0

2. "Procedures and Conditions for Inspection of Records", Ind. Code Ann. sec. 9-1-1-8

Maine

1. "Data Processing and Central Computer Service", Me. Rev. Stat. Ann. tit. 5, sec. 1851

Massachusetts

1. "Fair Information Practices", Mass. Gen. Laws Ann. ch. 66A

Minnesota

1. "Collection, Security and Dissemination of Records", Minn. Stat. Ann. sec. 15.162*

Oklahoma

1. "Confidentiality of Information Stored in Data Processing Center", Okla. Stat. Ann. tit. 74, sec. 118.17

Utah

1. "Information Practices", Utah Code Ann. sec. 63-50-1

Washington

1. "Confidential or Privileged Information", Wash. Rev. Code sec. 43.105.070

F. Trade Secrets

California

1. "Disclosure of Trade Secrets", Cal. Penal Code sec. 499C

Illinois

1. "Property", Ill. Ann. Stat. ch. 38, sec. 15-1

Massachusetts

1. "Crimes Against Property", Mass Gen. Laws Ann. ch. 226, sec. 30

Minnesota

1. "Theft and Related Crimes", Minn. Stat. Ann. tit. 40, sec. 609.52*

New Hampshire

1. "Consolidation", N.H. Rev. Stat. Ann. sec. 637:1

New York

1. "Offenses Involving Theft", N.Y. Penal Law ch. 46, sec. 155.00*
2. "Grand Larceny in the Third Degree", N.Y. Penal Law ch. 46, sec. 155.30*
3. "Unlawful Use of Secret Scientific Material", N.Y. Penal Law ch. 46, sec. 165.07

Oklahoma

1. "Larceny of Trade Secrets", Okla. Stat. Ann. tit. 21, sec. 1732

Tennessee

1. "Trade Secrets", Tenn. Code Ann. sec. 39-4238

G. Educational Records

Delaware

1. "Disclosure of Pupils' School Records", Del. Code Ann. tit. 14, sec. 4111

Florida

1. "Procedures for Maintenance and Transfer of Pupil Records", Fla. Stat. Ann. 232.23

Illinois

1. "Illinois School Student Records Act", Ill. Ann. Stat. ch. 122, sec. 50-1

Iowa

1. "Confidential Records", Iowa Code Ann. sec. 68A.7*

Maryland

1. "Conditions and Exceptions for the Inspection of Public Records", Md. Ann. Code art. 76A, sec. 3

Michigan

1. "Disclosing of Students' Communications by School Employees", Mich. Comp. Laws Ann. sec. 600.2165*

Mississippi

1. "Keeping and Use of Records", Miss. Code Ann. sec. 37-15-3

Oklahoma

1. "Information Concerning Pupil", Okla. Stat. Ann. tit. 70, sec. 6-115

H. Others

California

1. "Confidential Records, Rules and Regulations", Cal. Welf. & Inst. Code sec. 10850
2. "Title 1.82 Business Records", Cal. Civ. Code sec. 1799

Connecticut

1. "Arrest Record on Job Application Form", Conn. Gen. Stat. Ann. sec. 31-51i

Delaware

1. "Violation of Privacy; Class A Misdemeanor", Del. Code Ann. tit. 11, sec. 1335*

Hawaii

1. "Civil Identification", Hawaii Rev. Stat. sec. 28-34 et seq.

Illinois

1. "Data Information Systems Commission", Ill. Ann. Stat. ch. 127, sec. 1201

Massachusetts

1. "Confidentiality of Reports of Injured Children", Mass. Gen. Laws Ann. ch. 119, sec. 51E

2. "Public Assistance Records; Public Inspection; Destruction", Mass. Gen. Laws Ann. ch. 66, sec. 17A*

3. "Right of Privacy", Mass. Gen. Laws Ann. ch. 214, sec. 1B*

4. "Papers Concerning Adoption; Segregation and Inspection", Mass. Gen. Laws Ann. ch. 210, sec. 5C

Minnesota

1. "Polygraph Tests of Employees or Prospective Employees Prohibited", Minn. Stat. Ann. sec. 181.75

North Carolina

1. "Privacy of Employee Personnel Records", N.C. Gen. Stat. sec. 153A-98

2. "Privacy of Employee Personnel Records", N.C. Gen. Stat. sec. 160A-168

North Dakota

1. "Release of Information by Highway Commissioner", N.D. Cent. Code sec. 39-06-03.1

Wisconsin

1. "Right of Privacy", Wis. Stat. Ann. sec. 895.50

APPENDIX "F"

UPDATE ON RECENT STATE COMPUTER

RELATED CRIME LEGISLATION*

STATE	STATUS	BILL
ALABAMA	NONE	--
ALASKA	NONE	--
ARIZONA	BILL PASSED	H.B. #2212: Defines types of computer crimes and specified if first or second degree. Original bill and one passed are identical in nature. No change. PENALTY: Felony--5 years first degree, 1 1/2 years second degree. No mention of fine imposed.
ARKANSAS	NONE	--
CALIFORNIA	BILLED PASSED	H.B. #.66: The bill would make it a crime to directly or indirectly use a computer, computer system or network for a crime. Amendment added to include programmable pocket calculators. PENALTY: 16 months to 3 year prison sentence, $2,500-$5,000 fine, or both.

*This update is accurate through the time of this writing (fall, 1980). Given the fact that legislative activity is ongoing in many States, the status of certain bills listed here as pending may now have changed. Other bills in other States also may have been introduced.

STATE	STATUS	BILL
COLORADO	BILL PASSED	H.B. #1110: Similar to Florida bill. This bill defines the specifics of a computer system. PENALTY: Damages less than $50--class 3 misdemeanor. Damages more than $50 but less than $200--class 2 misdemeanor. Damages more than $200 but less than $10,000--class 4 felony. Damages $10,000 or more--class 3 felony.
CONNECTICUT	BILL DID NOT PASS	H.B. #6034: The bill was very similar to the proposed Mass. Computer Crime Bill. It also addresses trade secrets which have not been in most of the new legislation that we are witnessing these days. The bill is a good start. PENALTY: Damages greater than $200 but less than $1,000--class D felony. Damages greater than $1,000--class B felony.
DELAWARE	NONE	--

STATE	STATUS	BILL
FLORIDA	BILL PASSED	H.B. #1305: Very clearly defines types of computer crimes. It also addresses trade secrets. PENALTY: Damages greater than $200 but less than $1,000--3rd degree felony. Damages in excess of $1,000 2nd degree felony. Stiff imprisonment terms: 1-5 years.
GEORGIA	NONE	--
HAWAII	TO BE RECONSIDERED IN 1981	H.B. #S.504: Computer Crimes. Introduced 02/06/79, referred to Judiciary Cmte. Carried over to 1980. No Felony.
IDAHO	NONE	--
ILLINOIS	BILL PASSED	H.B. #H.1027: Very similar to S.240. Illegal to alter computer programs without consent of owner. PENALTY: Services obtained, $1,000 or less--class A misdemeanor. Services obtained, more than $1,000--class 4 felony.
INDIANA	NONE	--

STATE	STATUS	BILL
IOWA	NONE	--
KANSAS	NONE	--
KENTUCKY	NONE	--
LOUISIANA	NONE	--
MAINE	NONE	--
MARYLAND	BILL DID NOT PASS	S.B. #893: Prohibits fraud by use of a computer, defines certain terms, establishes penalties, provides a certain exception and generally relates to fraud by use of a computer. PENALTY: Any person convicted under the provisions of this bill is guilty of a felony and is subject to imprisonment for not more than 10 years or a fine of not more than $10,000 or both.
MASSACHUSETTS	BOTH BILLS DID	H.B. #H.4782: A bill relating to establishing a computer privacy law. Introduced 01/03/79, referred to the Judiciary Committee. Adverse report accepted 04/17/79.

STATE	STATUS	BILL
MASSACHUSETTS (continued)		H.B. #911: This is a simplistic type of bill. Defines access to computer, computer network, program, software property. Very short. PENALTY: Felony--imprisonment not more than 10 years or a fine of not more than $5,000 or both.
MICHIGAN	BILL PASSED	H.B. #4112: A bill to Prohibit computer fraud. Well defined bill. Access, they specify as, to use the of a computer. PENALTY: If the violation involves $100 or less, the person is guilty of a misdemeanor. If the violation involves more than $100, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of no more than $5,000 or both.
MINNESOTA	BILL DID NOT PASS	H.B. #1003: Strongest legislation to date. Defines types of computer crimes and varying penalties that apply.
MISSISSIPPI	NONE	--

STATE	STATUS	BILL
MISSOURI	TO BE RECONSIDERED IN 1981	H.B. #711: Relating to computer systems, networks, equipment and supplies with penalty provisions. Introduced 01/03/79, referred to Criminal Jurisprudence Cmte. 01/08/79. Passed Senate 04/04/79. To House Judiciary Cmte. 04/25/79. Very well written. Has not been passed to date. PENALTY: Damages greater than $200 but less than $1,000--class D felony. Damages greater than $1,000--class C felony. NOTE: H.B. #771 is identical to H.B. #230 previously filed by Murray & Caskey.
MONTANA	NONE	--
NEBRASKA	NONE	--
NEVADA	NONE	--
NEW HAMPSHIRE	NONE	--
NEW JERSEY	NONE	--

STATE	STATUS	BILL
NEW MEXICO	BILL PASSED	H.B. #S.8: An act making misuse of computer a crime. It also addresses unauthorized computer use. PENALTY: $100 or less--petty misdemeanor. More than $100 but less than $2,500--4th degree felony. Value more than $2,500--3rd degree felony.
NEW YORK	NEW LEGISLATION INTRODUCED IN SEPT., 1980	A.B. #10141: The bill deals with computers owned or leased by State or local Governments. A quick survey of several Government offices and agencies revealed that not one had a formal, on-going centrally directed computer security program to provide adequate protection for the integrity and confidentiality of personal and other sensitive information. Records of the Dept. of Audit and Control indicate that at the State level alone, there are at least 980 points of access to the computer systems used by the State. This type of legislation was encouraged by the American Bar Association at its August 1979 meeting.

STATE	STATUS	BILL
NEW YORK (continued)		PENALTY: Computer fraud is a class D felony punishable by a fine not to exceed two and one half times the amount of the defendant's gain from said violation. Computer damage or destruction is a class E felony punishable by a sum not to exceed $50,000.
NORTH CAROLINA	Pending	H.B. #S.397: A bill making a computer related crime a felony. Classifies the physical damage to a computer as a computer crime in addition to illegally accessing a computer system or network. PENALTY: Specifies denial of a computer service to an authorized user guilty of a misdemeanor. Extortion--verbal or written communication is guilty of a felony.
NORTH DAKOTA	NONE	--
OHIO	NONE	--
OKLAHOMA	NONE	--
OREGON	NONE	--
PENNSYLVANIA	BILL UNDER CONSIDERATION	H.B. #H.1824: Legislation dealing with computer crime. Introduced 10/11/79, referred to the Judiciary Committee.

STATE	STATUS	BILL
RHODE ISLAND	BILL PASSED	H.B. #5775: Follows format of pending California legislation. Also, it does not include microwave communications in the definition of "computer network". Specifies intentional access/alteration, damage or destruction. PENALTY: Felony--individual shall be fined not more than $5,000 or imprisoned for not more than five (5) years, or both.
SOUTH CAROLINA	BILL DID NOT PASS	H.B. #2821: An act making misuse of computers a crime.
SOUTH DAKOTA	BILL PASSED AWAITING SIGNATURE	H.B. #H.1292: A bill to establish property rights and penalties in computer programs, data and electronic communications. Introduced 1/17/80, referred to Local Government Committee 2/6/80. First reading in Senate, 2/5/80, second reading in House PASSED with title amended. 2/12/80 PASSED Senate as amended. 2/14/80 to Governor.
TENNESSEE	NONE	--
TEXAS	NONE	--
UTAH	BILL PASSED	H.B. #183: Computer Fraud Act. Very well written. Addresses services, property, computer network, computer access, financial

STATE	STATUS	BILL
UTAH (continued)		instrument, software or program. PENALTY: Damages less than or equal to $25--class C misdemeanor. Damages greater than $25, but less than or equal to $100--class B misdemeanor. Damages greater than $100 but less than or equal to $300--class A misdemeanor. Damages greater than $300 but less than or equal to $1000--3rd degree felony.
VERMONT	NONE	--
VIRGINIA	NONE	--
WASHINGTON	NONE	--
WEST VIRGINIA	NONE	--
WISCONSIN	NONE	--
WYOMING	NONE	--

APPENDIX "G"

SUMMARY OF THE FEDERAL COMPUTER

SYSTEMS PROTECTION ACT (S.240)

On January 25, 1979, Senator Abraham Ribicoff (D-Conn.) introduced the "Federal Computer Systems Protection Act of 1979". The bill contained a preamble which states that computer crime is a "growing problem" in the governmental and private sectors; that many opportunities exist for such crimes to be committed, at great expense to the public; and that current criminal statutes make prosecution of computer crime felons "difficult".

The bill proposed that the U.S. Criminal Code be amended to include Section 1028, entitled "Computer Fraud and Abuse". This section would reach all Government computers, computers used by private businesses operating under Government contracts, computers employed in the banking and finance industries, and computers used by any "entity" operating in or affecting interstate commerce.

The bill defined commonly used computer terminology and encompassed these terms in its "computer fraud and abuse" proscriptions. These include definitions for "access"; "computer"; "property"; "services"; "financial instrument"; "computer program"; and "computer software". The bill proscribed any use of a computer for fraudulent purposes and "intentional, unauthorized use, access to or alterations of a computer, computer program or data".

Penalties for violating the proposed law ranged from (a) 15 years imprisonment and/or a fine of two-and-one-half times the amount stolen, to (b) 15 years imprisonment or a $50,000 fine, or both.

☆U.S. GOVERNMENT PRINTING OFFICE: 1981-341-233/1392

END