Prosecuting Computer-Related Crime in the United States, Canada, and England: New Laws for Old Offenses

Lisa A. Menelly
Prosecuting Computer-Related Crime in the United States, Canada, and England: New Laws for Old Offenses?

I. INTRODUCTION

"Information - unlike food, shelter, health, or energy, is not a primary factor to human survival. It is, however, necessary immediately after these basic factors . . . ."1

Computers have become an integral part of modern industrial societies, utilized in almost every aspect of human endeavor.2 While the increased use of computers has extended the benefits of advanced technology to society,3 computers have also created a new avenue for criminal activity.4 Crimes involving the use of computers have increased at a substantial rate,5 prompting national debate over the need for specific legislation to combat this twentieth-century problem.6

Several factors, such as the growing availability of personal computers7 and heightened computer literacy,8 have contributed to the increase in computer-related crime. Much of the increase, however, is due to advances in networking, a method of accessing computer systems via dial-in facilities.9 With the use of a

2. See Sokolik, Computer Crime - The Need for Deterrent Legislation, 2 COMPUTER L.J. 353, 355 (1980) (stressing that the computer has become the "workhorse" of data processing: "[s]ociety could not revert to the days of manual processing of information even if it wanted to do so").
3. Computer industry projections in the United States indicate that in the home market alone, over 80 million personal computers will be in existence in 1990, as compared to only 5000 in 1978. 130 CONG. REC. H7631 (daily ed. July 24, 1984).
8. Computer terminals are a common feature in the classroom, even at the elementary school level. Thornton, supra note 7.
modem, a device which allows computers to "communicate" over telephone lines, home computers can be connected to computer systems worldwide.\(^\text{10}\)

Computer-related crime is often divided into four categories: introduction of fraudulent records or data into a computer; alteration or destruction of computer data or files; theft of money, financial instruments, property, services, or valuable data; and unauthorized use of a computer.\(^\text{11}\) Canadian and U.S. media coverage of computer-related crimes has primarily focused on perpetrators of the fourth category of computer-related crime, the unauthorized users or "hackers"\(^\text{12}\) who gain access to a computer system,\(^\text{13}\) often for the challenge of "breaking in."\(^\text{14}\)

In one illustrative incident,\(^\text{15}\) several youths in the United States used home computers to break into the computer files of a major cancer research center, where they altered patient records and radiation doses.\(^\text{16}\) This incident clearly demonstrates that unauthorized computer use is more than mere "intellectual pranksterism."\(^\text{17}\) The risks surrounding unauthorized computer use involve international concerns ranging from threats to national security\(^\text{18}\) to increasing monetary losses due to computer-related crime.\(^\text{19}\)

In the United States, formal efforts to make computer-related crime a federal offense began in 1977, with the introduction of the Federal Computer Systems Protection Act.\(^\text{20}\) Had the Act passed,\(^\text{21}\) it would have broadly prohibited any

---

10. Id. See also Thornton, supra note 7.
12. See, e.g., Thornton, "Hackers" Ignore Consequences of High-Tech Joyrides, Washington Post, May 21, 1984, cited in 129 CONG. REC. S6524 (daily ed. May 24, 1984) [hereinafter cited as Thornton II]. The article mentions, for example, an incident where students at the Dalton school in Manhattan used their classroom computers to break into 21 computer systems in Canada.
13. The U.S. General Accounting Office's definition of computer system is comprehensive, including not only computer hardware and computer programs (software), but also organizations and procedures for preparing input to the computer and using the output. General Accounting Office, Computer-Related Crimes in Federal Programs, 1 (1976).
14. The Criminal Justice Newsletter notes that "hacking" has become a familiar term to the criminal justice professional. The Newsletter defines "hacking" as cracking codes and breaking into computer systems, either "for mischief or malice." Crim. Just. Newsletter, June 20, 1983, at 4, col. 2.
15. Thornton II, supra note 12, at S6524.
17. House Report, supra note 4, at 11. The House Report indicated that the U.S. public downplays the seriousness of computer-related crime, creating an "attitudinal problem" in preventing the offense. Id. at 12.
18. In Canada, much of the media coverage on hacking has focused on the threat to national security. See Webber, Computer Crime or Jay-walking on the Electronic Highway, 1983 CRIM. QTLY 217, 218.
fraudulent or intentional unauthorized use of a computer system.\textsuperscript{22} Until recently, however, Congress has been hindered in its attempt to pass criminal legislation by disputes over the question of what constitutes a computer crime.\textsuperscript{23} Congress now has chosen to define computer-related crime as specific acts, such as the gaining of access to a computer facility without authorization.\textsuperscript{24} In contrast, computer expert Donn Parker defines computer-related crimes by focusing on the role of the computer in a given crime.\textsuperscript{25} Computer expert John Taber argues that “computer crime,” per se, does not exist.\textsuperscript{26} According to this view, the computer is merely a new tool for committing established crimes, such as embezzlement or theft.\textsuperscript{27}

As a result of these varying viewpoints, strong disagreement exists over the need for legislation prohibiting computer usage for criminal purposes.\textsuperscript{28} Opponents of computer-specific legislation argue that traditional statutes, such as fraud or theft statutes, are adequate to secure convictions for crimes involving computers.\textsuperscript{29} Deputy District Attorney Donald Ingraham has argued that if computer crime legislation is enacted, it should clearly state that it does not pre-empt the use of other statutes which may be more appropriate for prosecution.\textsuperscript{30} Despite the disagreements, the 98th Congress, spurred on by dramatic increases in “hacker” incidents,\textsuperscript{31} enacted the nation’s first federal computer crime legislation, The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.\textsuperscript{32}

\begin{itemize}
\item \textsuperscript{21} The bill failed to report out of the Senate Committee on the Judiciary at the end of the second session.
\item \textsuperscript{22} S. 1766, introduced by Senator Ribicoff in 123 Cong. Rec. 10,790 (1977).
\item \textsuperscript{23} See Hearings on H.R. 3970 (Federal Computer Systems Protection Act) Before the Subcomm. on Civil and Constitutional Rights of the Comm. on the Judiciary, 97th Cong., 2nd Sess. 63, 64 (1982) (describing and criticizing existing computer crime definitions) [hereinafter cited as Hearings on H.R. 3970].
\item \textsuperscript{24} See supra note 11 and accompanying text.
\item \textsuperscript{25} Hearings on H.R. 3970, supra note 23, at 46. (Statement of D. Parker). Parker identifies four possible roles that a computer could play in a computer-related crime. These include: 1) the computer as the object of a physical attack (e.g. vandalism); 2) the computer as a “unique form of assets subject to abusive acts” (e.g. programs); 3) the computer as an “instrument” or tool for planning a crime; 4) the computer as a symbol to intimidate or deceive (e.g. a fraudulent investment scheme involving a “secret computer program” guaranteed to predict stock market activity).
\item \textsuperscript{26} Taber, supra note 6, at 518-26.
\item \textsuperscript{27} Id. at 537.
\item \textsuperscript{28} See supra note 6 and accompanying text.
\item \textsuperscript{29} See Hearings on S. 240 Before the Subcomm. on Criminal Justice of the Comm. on the Judiciary on S. 240, 96th Cong., 2nd Sess. 1, 5-16 (1980) [hereinafter cited as Hearing on S. 240].
\item \textsuperscript{30} Ingraham, On Charging Computer Crime, 2 COMPUTER LJ. 429, 438 (1980).
\item \textsuperscript{31} The increased number of “hacker” incidents is due to advances in computer networking. See supra notes 10-11 and accompanying text.
In Part II of this Comment the author analyzes the approaches to computer-related crime in Canada and England. Recent Canadian cases have characterized computer programs and information as "property."\(^{33}\) Using this expanded definition of "property," Canadian courts have dealt with computer-related crimes under traditional fraud or larceny statutes.\(^{34}\) In England, courts have broadly interpreted provisions of the Theft Act to prosecute computer-related crimes.\(^{35}\) Neither country has enacted computer crime legislation. In Part III the author summarizes the major provisions of the new U.S. Computer Fraud and Abuse Act, and discusses enforcement issues surrounding unauthorized access to computers and theft of computer software. The author compares the prosecution of computer-related crimes under the Computer Fraud and Abuse Act with prosecution under other applicable statutes in the United States. Part IV of this Comment addresses the need for computer system security, in addition to criminal statutes, to deter computer-related crime. The Small Business Computer Security and Education Act of 1984,\(^{36}\) recently enacted in the United States, encourages this preventive approach by enabling the Small Business Administration\(^{37}\) to disseminate information on management techniques and computer system security. In Part V, the author compares and contrasts the U.S., Canadian, and English approaches to computer-related crimes, focusing on the status of information within the definition of property for each country. The author concludes that a better understanding of the roles of information and technology is necessary as a basic weapon in combatting computer-related crime.

II. COMPUTER-RELATED CRIME IN CANADA AND ENGLAND

A. Canada

As in the United States, an increasing number of "hacker" incidents has intensified the pressure for computer-related criminal legislation in Canada.\(^{38}\) Although Canada has yet to enact any national computer legislation, one recently proposed bill\(^{39}\) would have expanded the definition of property to include

---

33. See infra text accompanying notes 60-83.
34. Id.
35. See infra text accompanying notes 90-98.
37. The Small Business Administration was established in 1958 to further the congressional goals of aiding and counseling small business concerns. The operation of small business development centers is one function of the Small Business Administration. See 15 U.S.C. \$ 631-649 (1982).
38. See Webber, supra note 18.
intangibles and would have created a new offense for tampering with a computer.41

Much of the controversy over the need for computer crime legislation has resulted from the 1980 case of Regina v. McLaughlin.42 McLaughlin, a student at the University of Alberta, had gained access to university computer files without authorization, and obtained internal programs and data.43 In the Trial Division,44 the Supreme Court of Alberta convicted McLaughlin of theft.45 Expanding § 287 of the Canadian Criminal Code,46 the court held that a computer was a telecommunications facility within the meaning of the statute.47 The Appellate Division subsequently reversed the holding of the Alberta Supreme Court, based on a strict interpretation of the statute.48

The Supreme Court of Canada affirmed the judgment of the Appellate Division.49 In a concurring opinion, Justice Estey reasoned that § 287 was directed primarily at broadcasting and telephone interception,50 and concluded that if Parliament had intended to have penal consequences for unauthorized computer use, it could have done so specifically by including the term "computer" in a penal statute.51 He further stated that the Court would not interpret a statute directed at the communications industry as also intending to proscribe

40. Bill C-667, supra note 39, would have amended the definition of "property" in § 385 to include "any computer software or program, or copy thereof, in any retrieval computer data or information produced and stored in a machine readable form by any means."
41. Bill C-667, supra note 39, Section 387.1 (Mischief) provided that:

   Every one commits mischief who wilfully (a) destroys or damages property; (b) renders property dangerous, useless, inoperative or ineffective; (c) and without authorization, express or implied, destroys or damages a computer program or computer data or alters a computer program or data in a way that renders it useless or inoperative or diminishes its commercial or scientific value; (d) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property . . . .

42. 18 Criminal Reports [C.R.] 3d 339 (1980), 53 Canadian Criminal Cases [C.C.C.] 2d 417, One commentator believes that this decision is the single most important factor in the current computer crime controversy. See Webber, supra note 18.
43. Regina v. Christensen, reported in 26(10) Chitty's L.J. 348 (1978). (McLaughlin was convicted with two other students. Only McLaughlin appealed the conviction.)
44. The court system in Canada is comprised of provincial and federal courts. The federal courts consist of a Trial and an Appellate Division. The Supreme Court of Canada hears appeals from both provincial and federal courts.
45. 26(10) Chitty's L.J. at 353.
46. Criminal Code, CAN. REV. STAT. 1970, ch. C-34, § 287(1)b (re-enacted 1974-75-76, ch. 93, § 23) reads as follows: "287(1) Every one commits theft who fraudulently, maliciously, or without colour of right . . . (b) uses any telecommunication facility or obtains any telecommunication service." Subsection (2) (re-enacted 1974-75-76, ch. 93, § 23) defines "telecommunication" as "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio by natural, electronic or other electromagnetic system."
47. 26(10) Chitty's L.J. at 350.
49. 18 C.R. 3d 399.
50. 18 C.R. 3d at 345-349 (Estey, J., concurring opinion).
51. Id. at 349.
the unauthorized operation of a computer, and indicated that such change should come from the legislative branch.52

Even though the McLaughlin case rendered § 287 inapplicable to unauthorized access to a computer, other Canadian statutes have allowed convictions for such crimes.53 In Regina v. Marine Resource Analysts Ltd.,54 the defendant used a password belonging to his previous employer, the Department of Fisheries, to gain access to the computer facility of the University of New Brunswick.55 Based on the password, the University billed the Government of Canada for the computer time.56 Cleared of the charge under § 287,57 the defendant was convicted under § 42158 of attempting to defraud the government.59

In the 1982 case of Regina v. Stewart,60 the Ontario Court of Appeal held that copying a confidential list of hotel union employees from a computer printout constituted theft of property.61 Under § 283(1)d of the Canadian Criminal Code, theft includes converting property with intent to use it in such a way that it cannot be restored to the owner in its original condition.62

Reversing a dismissal by the trial court,63 the Court of Appeal first determined that confidential information acquired by a commercial enterprise through an expenditure of labor and money constituted property under § 283.64 Reasoning that when confidential property is copied it loses its value to the owner, the court found the requisite intent under § 283(1)d.65

In a lengthy dissent, Justice Lacourciere argued that the extension of the concept of "property" to include information is a task reserved for the legisla-
The Justice noted that proposed amendments to § 283 of the Criminal Code would specifically include computer programs and data in the definition of property. His dissent asserts that the judiciary is not the appropriate forum in which to expand the definition of property. Reiterating the reasoning of the trial court, Justice Lacourciere stressed that if the current interpretation of property was not adequate for the needs of modern Canadian society, "the remedy must be a change in the law by Parliament." His dissent reflects a growing concern with the necessity of expanding traditional property concepts.

In the most recent Canadian case involving computer-related crime, Turner and the Queen, the Ontario High Court reconciled the absence of Parliamentary action with judicial expansion of the definition of property. In Turner, the defendants had accessed computer tapes and tampered with the program stored on the tapes so that other users were unable to use the program without first obtaining the new program code. The Turner court, in order to affirm a conviction under § 387, the mischief offense, had to find an interference with the use or operation of "property".

Urging strict statutory interpretation, the defendants argued that the mischief offense, as currently enacted, did not prohibit the alteration of electronic data. Although admitting to altering the data, the defendants denied any interference with "property," reasoning that the computer tape itself was not physically damaged, and was still usable as a storage tape. Pointing to proposed amendments which would specifically prohibit the alteration of data, the defendants

66. Id. at 235.
67. Id. at 230. See Bill C-667, supra note 39 and accompanying text.
68. 42 Ont. 2d at 230, 235.
69. Id. at 230 (quoting Keever, J., in Regina v. Stewart, 38 Ont. 2d 84, 95 (1982)).
70. A similar concern exists in the United States. Commenting on the Computer Fraud and Abuse Act, Congressman Rodino stated that "[t]he Federal law must keep pace with technology. It is as important today to develop Federal protection for intangible property such as information . . . as it was to develop Federal law to protect tangible assets in interstate commerce in the past." 130 Cong. Rec. H7635 (daily ed. July 24, 1984).
72. Id. at 434.
73. Id. at 431.
74. In pertinent part, § 387(1) of the Canadian Criminal Code provides that "[e]very one commits mischief who wilfully . . . (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property."
75. 13 C.C.C. 3d at 433. Under § 385, the applicable definition section for the mischief offense, "property" is defined as "real or personal corporeal property." Section 385 of the Canadian Criminal Code.
76. 13 C.C.C. 3d. at 433.
77. Id. at 433-34.
78. Bill C-19, An Act to Amend the Criminal Code, 32nd-33d Legis., Eliz. II, 1983-84, proposed enactment of new subsection 387(1.1) provided that:

Every one commits mischief who wilfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or,
argued that the amendments clearly indicated Parliament had not intended for the current mischief offense to apply to alteration of data.\(^79\)

Rejecting this argument, the Turner court held that interference with the enjoyment of property was the essence of the mischief offense.\(^80\) The Turner court found that the defendants, by their actions, had interfered with the retrieval of data off the tape, making it impossible for other users to process their work.\(^81\) The court referred to the definition of property as interpreted by the Stewart court,\(^82\) and concluded that the Parliamentary intent, as indicated by the proposed amendments, was not to alter § 387, as urged, but rather to clarify the existing law.\(^83\) If the Turner case is followed, Canadian courts will treat alteration or destruction of computer data specifically as an interference with property.

B. England

England has also been plagued by the problem of whether intangibles such as information should be considered property. The leading case in this area is Oxford v. Moss,\(^84\) in which a student obtained a paper copy of examination questions, read the questions and returned the paper.\(^85\) The Oxford court held that the abstraction of confidential information was not theft of intangible property for purposes of the Theft Act 1968.\(^86\)

Several commentators have argued that this holding should not extend to information stored in a computer, as this information deserves the protection of criminal law.\(^87\) English courts dealing with computer-related crimes have neatly skirted the information debate by framing the computer’s role in a crime in terms of its use as a new tool or method for accomplishing an established crime.\(^88\) Indeed, whenever possible, English courts have analogized computer-related crimes to more recognizable fact patterns.\(^89\) In this way, the courts also avoid entanglement in such issues as unauthorized access.

The 1984 case of Regina v. Thompson,\(^90\) vividly illustrates the English approach

---

\(^{79}\) See supra text accompanying notes 60-65.

\(^{80}\) Id. at 434.

\(^{81}\) Id.

\(^{82}\) Id. at 435.

\(^{83}\) Id. at 185.

\(^{84}\) 68 Crim. App. 183 (1978).

\(^{85}\) Id. at 185.

\(^{86}\) Id. at 185-86.

\(^{87}\) See, e.g., Tettenborn, Stealing Information, 129 NEW L.J. 967 (1979); C. TAPPER, COMPUTER LAW 216 (3d ed. 1983).

\(^{88}\) See infra notes 90-98 and accompanying text.

\(^{89}\) Id.

\(^{90}\) [1984] 1 W.L.R. 962.
to computer-related crime. Thompson, a computer operator, had entered dormant bank account files, recorded withdrawals, and credited his own account with the money.\textsuperscript{91} The transfers had occurred in the computer files of a bank in Kuwait.\textsuperscript{92} Thompson was apprehended in England while attempting to have the money sent to a local bank.\textsuperscript{93} Affirming Thompson's conviction of theft,\textsuperscript{94} the Leed's Court of Appeal stated:

Discard for the moment the modern sophistication of computers and programmes and consider the old days when bank books were kept in manuscript in large ledgers. In effect all that was done by the appellant was to take a pen and debit each of the five accounts in the ledger with the relevant sums and then credit each of his own five savings accounts in the ledger with corresponding amounts.\textsuperscript{95}

Another English Court of Appeal had used similar reasoning in the 1981 case of \textit{Regina v. Davies & Nocross}.\textsuperscript{96} Nocross, a brewery employee, had deleted orders on computer files so that Davies received beer without being billed.\textsuperscript{97} The court stated that it was unnecessary to determine the details or technicalities of how the fraud was accomplished, noting simply that the result of the activity was non-payment for deliveries.\textsuperscript{98}

The English courts' expanded use of existing laws has helped combat at least those computer-related crimes which end in accomplishing traditional crimes, such as conversion and fraud. The courts' focus on the results of computer-related crimes has allowed English courts to prosecute such crimes without resort to specific computer crime legislation. Computer-related crimes such as the theft of computer programs, however, are not so easily adapted to prosecution under existing laws.

Although the theft of information is not specifically prohibited under English law,\textsuperscript{99} Professor Tettenborn of the University of Nottingham has argued that the offense of obtaining a service or "benefit" by deception is applicable to the theft

\begin{itemize}
  \item \textsuperscript{91} Id. at 964.
  \item \textsuperscript{92} Id.
  \item \textsuperscript{93} Id.
  \item \textsuperscript{94} Thompson was convicted under § 15 of the Theft Act of 1968, which states:
    \begin{enumerate}
      \item A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it . . . .
      \item For purposes of this section a person is to be treated as obtaining property if he obtains ownership, possession or control of it, and "obtain" includes obtaining for another or enabling another to obtain or to retain.
    \end{enumerate}
  \item \textsuperscript{95} 1 W.L.R. at 964.
  \item \textsuperscript{96} C. A. (Crim.Div.) No. 90/CI/80, (1981) (available Nov. 21, 1984, on LEXIS, Enggen library, Cases file). The defendants had appealed to reduce their sentences on their conviction for fraud.
  \item \textsuperscript{97} Id.
  \item \textsuperscript{98} Id.
  \item \textsuperscript{99} See supra notes 84-88 and accompanying text.
\end{itemize}
of computer data or programs. By equating “information” with “benefit”, Tettenborn reasoned obtaining information by deception is within the definition of the offense. The utility of the statute is limited, however, to situations where the “benefit” is provided with the expectation of payment. This additional requirement effectively precludes conviction of theft for the majority of computer programs which are generally not offered for sale.

The absence of computer crime legislation may be due to efforts of the English Law Commission, whose function it is to review various areas of the law and propose developments or reform. In a 1974 report, the Law Commission concluded that various provisions of the Theft Act are applicable to misuse of a computer to secure money or goods, associated schemes to defraud, and false accounting. This expansive interpretation of existing provisions in the Theft Act has allowed prosecutors to treat as immaterial the fact that the defendant used computer technology to accomplish the crime.

Both English and Canadian courts to date have successfully prosecuted computer-related crimes without resort to computer crime legislation by broadly interpreting existing statutes. By contrast, the United States has recently chosen to enact specific computer crime legislation.

III. Computer-Related Crime in the United States

In an attempt to alleviate some of the problems in prosecuting computer-related crimes in the United States, and to deter the increasing number of

100. See Tettenborn, supra note 87. Section 1 of the Theft Act 1978 states:
101. See Tettenborn, supra note 87, at 967.
102. Id.
103. See text of § 1(2) of the Theft Act, 1978, supra note 100.
104. Tettenborn, supra note 87, at 967.
105. The Law Commissions Act, 1965 states:
107. See House Report, supra note 4, at 9, 10. The report states that one obstacle to prosecution is that much of the property involved in computer crimes, such as programs and data, does not fit within the definitions of property in traditional theft and larceny statutes. But c.f. infra text accompanying notes 187-190.
incidents of unauthorized access by hackers.\textsuperscript{108} Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Computer Fraud and Abuse Act).\textsuperscript{109} This section analyzes the major provisions of the Act, and assesses its potential effectiveness for prosecuting computer-related crimes.

A. The Definition and Scope of Criminal Acts Under the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act defines criminal acts of computer usage and provides sanctions for fraudulent or related activity in connection with computers.\textsuperscript{110} Towards this end, the Act delineates three categories of unauthorized access\textsuperscript{111} to computers. The first of these prohibited activities is any unauthorized access to obtain classified information\textsuperscript{112} with the intent to use such information either against the United States or to the advantage of another nation. The Act defines such unauthorized access as a felony.\textsuperscript{113}

The Act defines the two other categories of offenses as misdemeanors.\textsuperscript{114} The first of these lesser offenses is the unauthorized access by computer to information protected by either the Right to Financial Privacy Act\textsuperscript{115} or the Fair Credit Reporting Act.\textsuperscript{116} The other lesser offense only refers to computers used for or on behalf of the U.S. government, and involves unauthorized access which results in the use, modification, destruction, or disclosure of information in the

\textsuperscript{108} House Report, \textit{supra} note 4, at 4-5. The Committee on the Judiciary was concerned with the lenient public attitude towards the white collar nature of computer-related crime. The committee reasoned that criminal legislation would be a deterrent, and would provide the necessary guidelines for proscribed activity in this area.


\textsuperscript{110} Id.

\textsuperscript{111} As used in this article, the phrase "unauthorized access" encompasses the following language in the statute: "accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." 18 U.S.C.A. § 1030(a)(1)-(3) (West Supp. 1985).

\textsuperscript{112} 18 U.S.C.A. § 1030(a)(1) (West Supp. 1985) defines classified information as information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of § 11 of the Atomic Energy Act of 1954.

\textsuperscript{113} 18 U.S.C.A. § 1030(c)(1)(A) (West Supp. 1985). The felony provides for a fine of up to $10,000 (or twice the value obtained ) or for imprisonment up to ten years. Id.

\textsuperscript{114} 18 U.S.C.A. § 1030(c)(2)(A) (West Supp. 1985). The misdemeanors provide for a fine of up to $5000 (or twice the value obtained ) or for imprisonment up to one year. Id.


computer.\textsuperscript{117} This offense also involves any unauthorized access which would prevent the authorized use of a government computer.\textsuperscript{118}

In this last offense, the provisions relating to unauthorized use or disclosure of government information have already received much criticism, and may not be retained. Jerry Berman of the American Civil Liberties Union immediately attacked this portion of the Act, characterizing it as tantamount to a "government secrecy" law.\textsuperscript{119} Senator Mathias has argued that this section is, in effect, a broad anti-disclosure statute, prohibiting disclosure of information even when disclosure is mandated under the Freedom of Information Act.\textsuperscript{120} To reconcile this discrepancy, the Senator has proposed an amendment which will narrow the scope of the anti-disclosure provision to information protected by the Privacy Act.\textsuperscript{121} If such an amendment is not adopted by the 99th Congress, U.S. courts may soon be faced with the difficult task of integrating two statutes with conflicting aims.\textsuperscript{122}

Commentators have severely criticized previous computer crime bills for their failure to distinguish between unauthorized access for criminal purposes, such as fraud, and unauthorized access for personal work or frolic, such as game playing.\textsuperscript{123} The Computer Fraud and Abuse Act has made this distinction. The Act specifically excludes from its coverage computer-related activities which exceed the scope of authorization, but result only in the use of computer time.\textsuperscript{124} An example of excluded activity is the unauthorized use of a government computer by an employee to play games or to do homework.\textsuperscript{125} Such an activity is generally

\textsuperscript{118} Id.
\textsuperscript{119} 42(42) CONG. Q. 2752 (1984).
\textsuperscript{121} Senate bill S.610, which narrows this provision, was introduced by Senator Mathias on March 7, 1985. S.610, 99th Cong., 1st Sess. 131 CONG. REC. S2727 (daily ed. Mar. 7, 1985). Senator Mathias had proposed a similar amendment prior to enactment of the Computer Fraud and Abuse Act. 130 CONG. REC. 14,445 (daily ed. Oct. 11, 1984). This amendment passed in the senate but was rejected by the House of Representatives. The Privacy Act is codified at 5 U.S.C. § 552a (1982).
\textsuperscript{122} In a similar vein, Colin Tapper notes that the conflicting overlap of information covered under the Freedom of Information Act, 5 U.S.C. § 552 (1982), and the Privacy Act, 5 U.S.C. § 552a (1982), has yet to be judicially defined. He suggests that this task will provide "a difficult and fertile new field for litigation." TAPPER, supra note 87, at 111.
\textsuperscript{123} See, e.g., Taber, supra note 6, at 530-32; Comment, Legislative Issues in Computer Crime, 21 HARV. J. ON LEGIS. 259, 252-255 (1984) [hereinafter cited as Legislative Issues].
\textsuperscript{124} 18 U.S.C.A. § 1030(a) (West Supp. 1985) provides that
[\textquoteleft]it is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.\textquoteright
\textsuperscript{125} Id. See House Report, supra note 4, at 22.
considered to be "time stealing," and Congress intended it to be handled at the administrative level.  

In effect, the Computer Fraud and Abuse Act establishes a new category of crime where the use of a computer for criminal purposes is the criminal activity. This aspect of computer-specific legislation has not gone uncriticized. Senator Laxalt analogized the function of a computer to that of a filing cabinet and queried, "why should someone be treated differently for stealing information out of a filing cabinet than a person who takes the same information from a computer?" Congress has chosen, however, to treat the computerized form of information storage as a distinct kind of activity, in order to regulate its newly discovered uses and abuses.

At present, the Computer Fraud and Abuse Act regulates unauthorized access to government computers. For private computer systems, coverage under the Act extends only to those computers which contain certain financial or credit records, or information necessary to national security. Previous attempts at computer crime legislation would have regulated unauthorized access not only to government computers, but to any computer used by an entity operating in or affecting interstate commerce. An earlier version of the Computer Fraud and Abuse Act also followed this approach. Two proposed provisions from this early version would have extended coverage to all computer systems when the unauthorized access resulted in a loss of over $5000. Congress withdrew these provisions from the enacted version of the Computer Fraud and Abuse Act, and as a result, the prosecution of most computer-related crimes committed on private computer systems must proceed under other federal or state statutes.

B. Enforcement Issues Under the Computer Fraud and Abuse Act and Other Statutes

1. Supplementary Federal Statutes

Although the Computer Fraud and Abuse Act specifically addresses computer-related crimes, it is unclear whether existing statutes which allow prosecution based on the underlying crime may not be as effective. For prosecu-

126. Id.
128. One commentator suggests that prohibiting unauthorized access to a computer is equivalent to criminalizing unauthorized entrance into a records storeroom. Legislative Issues, supra note 123, at 252.
133. Id.
tion of computer-related crimes excluded from coverage under the Act, such as theft of computer time or unauthorized access to a private computer, the use of alternate statutes becomes essential. In recent years, federal prosecutors have applied over forty statutes to the prosecution of crimes involving computers.\textsuperscript{135}

The most commonly utilized statutes have been the federal mail and wire fraud statutes,\textsuperscript{136} and the federal theft statute.\textsuperscript{137}

Prior to the passage of the Act, several commentators had expressed concern that federal prosecutors were being forced to "shoe horn" computer-related offenses into existing statutes.\textsuperscript{138} Prosecutors were faced with the choice of drafting pleadings for statutes not originally designed to encompass computer-related activities, or allowing the activity to go unchallenged.\textsuperscript{139} In an address to Congress, John Keeney of the Department of Justice cited \textit{United States v. Seidlitz}\textsuperscript{140} as illustrative of this dilemma.\textsuperscript{141}

In \textit{Seidlitz}, the defendant used his office computer terminal in Virginia to fraudulently obtain software belonging to his previous employer, the Federal Energy Administration.\textsuperscript{142} The fact that two of the calls were made across state lines provided the only basis for federal jurisdiction under the wire fraud statute.\textsuperscript{143} Had the activities been within a single state, Seidlitz could not have been convicted.\textsuperscript{144}

The Computer Fraud and Abuse Act, on the other hand, does provide an independent basis for federal jurisdiction in such a case, since Seidlitz accessed a government computer without authorization.\textsuperscript{145} The penalties vary, however, between the two statutes. Under the new Act, the prosecutor is limited to seeking a one year imprisonment,\textsuperscript{146} in contrast to the five year sentence available under the wire fraud statute.\textsuperscript{147} If a prosecutor instead attempts to seek a higher fine

\begin{itemize}
  \item \textsuperscript{135} See Hearing on S. 240, \textit{supra} note 29, at 1.
  \item \textsuperscript{136} 18 U.S.C. § § 1341, 1343 (1982).
  \item \textsuperscript{137} 18 U.S.C. § 641 (1982).
  \item \textsuperscript{138} See, \textit{e.g.}, Sokolik, \textit{supra} note 2, at 373; \textit{Note, Computer Abuse: The Emerging Crime and the Need for Legislation}, 12 \textit{FORDHAM URB. L.J.} 73, 78 (1984) [hereinafter cited as \textit{Computer Abuse}].
  \item \textsuperscript{139} \textit{Computer Abuse}, \textit{supra} note 138, at 78, n. 36.
  \item \textsuperscript{141} \textit{House Report}, \textit{supra} note 4, at 6.
  \item \textsuperscript{142} 589 F.2d at 154, 155. Standard communications software packages enable computers to transmit and receive data and programs over telephone lines by the use of electronic signals.
  \item \textsuperscript{143} \textit{House Report}, \textit{supra} note 4, at 6.
  \item \textsuperscript{144} \textit{Id}.
  \item \textsuperscript{146} 18 U.S.C.A. § 1030(c)(2)(A) (West Supp. 1985).
  \item \textsuperscript{147} 18 U.S.C. § 1343 (1982) provides:

\begin{quote}
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.
\end{quote}

\textit{Id}.\end{itemize}
under the Computer Fraud and Abuse Act, he or she must consider the value the defendant obtained from the offense. For example, Seidlitz would have to have obtained a total value of over $2500 from the offense in order to increase the $5000 penalty set by the Act.\footnote{148} In addition, the Computer Fraud and Abuse Act is silent on whether the value of the use of computer time is included in calculating the total value obtained by the defendant from the commission of the crime.\footnote{149}

2. The Valuation of Computer Programs or Data

Where an offense consists essentially of the “theft” of programs or data, courts may face the thorny problem of determining the value of programs or data. This determination would be necessary in order to impose a stiffer penalty than the set fine or relatively short prison sentence provided for under the Computer Fraud and Abuse Act.\footnote{150} Although the Seidlitz court found that the transmitted data constituted “property” for purposes of the wire fraud statute,\footnote{151} it did not attempt to place a dollar value on the programs stolen, nor was it necessary to do so to determine an appropriate penalty.\footnote{152}

Although the Supreme Court of Alabama has allowed the use of development costs to determine the value of computer programs,\footnote{153} in other cases, the valuation of programs or data may be futile. One state court has held that when software such as a computer program has no predetermined market value, the preferred method of valuation is the use of actual value.\footnote{154} In that case, the software was obtained from a university computer in the form of computer printouts, and the printouts were assigned an actual value as scrap paper.\footnote{155} Given the problem of valuation under the Computer Fraud and Abuse Act, federal prosecutors facing a “theft” of programs may be able to obtain more

\footnote{148. 18 U.S.C.A. § 1030(c)(2)(A) (West Supp. 1985) specifies that the maximum fine is the greater of $5000 or twice the value obtained by the offense. These fines may be increased in 1986 in accordance with the provisions of the Sentencing Reform Act of 1984.}
\footnote{149. An early draft of the Computer Fraud and Abuse Act included a provision which specifically excluded the value of the use of computer time from the calculation of value obtained by the offense. See House Report, supra note 4, at 2-3. It is not yet known whether the final enactment of the law will be interpreted in a similar manner.}
\footnote{150. It should be noted, however, that one purpose of the Computer Fraud and Abuse Act was to avoid entangling courts in the issue of whether intangible property, such as a computer program, could be “stolen” when the owner remains in possession of the original. See House Report, supra note 4, at 9.}
\footnote{151. 589 F.2d at 160.}
\footnote{152. There are no dollar loss thresholds for the calculations of penalties under the mail fraud statute, 18 U.S.C. § 1341 (1982) or wire fraud statute, 18 U.S.C. § 1343 (1982).}
\footnote{153. National Surety Corp. v. Applied Systems, 418 So.2d 847, 850 (Ala. 1982).}
\footnote{155. 217 Va. at 692.}
appropriate penalties under a potentially applicable copyright, patent, or trade secret statute. 156

3. Prosecuting the Theft of Computer Time

Where an offense consists of the “theft” of computer time, prosecution may not be possible under the Computer Fraud and Abuse Act. The legislative history of the Computer Fraud and Abuse Act suggests that Congress intended the theft of computer time from private computers to be prosecuted under state or local law. 157 Prosecuting the theft of computer time, however, has confounded many state courts. 158 The Virginia case of Lund v. Commonwealth 159 illustrates this problem.

In Lund, the defendant had used over $26,000 in computer time. 160 The Supreme Court of Virginia reversed his conviction based on a strict interpretation of the state larceny statute, which did not include services as a proper object of larceny. 161 Although Virginia subsequently amended its larceny statute to include computer services, 162 many other states without such legislation are still unable to secure convictions for the theft of computer time.

Successful prosecution may not be possible even when a state larceny statute includes the theft of services. In People v. Weg, 163 the court held that New York’s larceny statute, which included theft of services, 164 did not apply to the unauthorized use of an employer’s computer. 165 The Weg court held that the theft of services applied only to services offered for sale, and did not apply to internal abuse of equipment. 166

At the federal level, the theft of computer time from a private employer has

156. An analysis of the legal remedies provided by copyright, patent, and trade secret law is beyond the scope of this article. For an excellent introduction into this area, see Davidson, Protecting Computer Software: A Comprehensive Analysis, 1983 Jurimetrics J. 337.
158. See text accompanying notes 159-66 infra.
159. 217 Va. 688.
160. Id. at 690. The computer used by the defendant was leased on an annual basis from IBM. The value of the computer time used was determined based on the rental cost. Id. at 689.
161. Id. at 691-2.
162. VA. CODE §§ 18.2-98.1 (1982). See also OHIO REV. CODE ANN. § 2901.01 (Baldwin 1984).
163. 450 N.Y.S.2d 957 (N.Y. City Crim. Ct. 1982).
164. Under the New York statute, a person commits theft of services when:

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

165. 450 N.Y.S.2d. at 959.
166. Id. at 960-61. The court also held that the computer was not commercial equipment because it was owned by the New York Board of Education. Id. at 958-9.
been successfully prosecuted under the federal mail fraud statute. In *United States v. Kelly*, the defendants used their employer’s computer to develop software for a personal business venture. The court held that the defendants’ use of computer time for personal benefit deprived the employer of honest and faithful services, and thus was a scheme to defraud within the meaning of the statute.

For the theft of computer time from a government computer, the legislative history of the Computer Fraud and Abuse Act suggests the use of administrative sanctions. Prior to enactment of the Act, federal prosecutors had used the larceny statute to prosecute the theft of computer time, as a thing of value belonging to the federal government. In *United States v. May*, the court adopted this use of the larceny statute to prosecute unauthorized personal use of government aircraft. The *May* court specifically rejected the argument that existing administrative sanctions precluded criminal sanctions and noted that Title 18 was not enacted to reconcile overlapping administrative and criminal remedies.

For the questionable criminal status of the theft of computer time under the Computer Fraud and Abuse Act, the existence of administrative sanctions should not preclude prosecution under the federal larceny statute. Prosecution of the theft of computer time under the federal larceny statute may also encourage state legislators and judges to broaden the definition of property within state larceny statutes.

---

169. Id. at 496-97.
170. Id. at 501. The court held that essence of the fraud was the loss to the employer of the employee’s "undivided loyalty in job performance" while in pursuit of concealed financial gain. Id.
172. 18 U.S.C. § 641 (1982) provides:
   Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof ... [s]hall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1000 or imprisoned not more than one year, or both.
174. Id. at 880. The *Sampson* court held that unauthorized use of over 190 hours of government computer time and use of storage facilities constituted "things of value" under the federal larceny statute. Id.
175. 625 F.2d 186 (8th Cir. 1980).
176. Id. at 190-92. The *May* court reversed the convictions and remanded on other grounds. Id. at 195.
177. Id. at 189.
178. Id.
179. For example, in the 1984 case of *United States v. Croft*, 750 F.2d 1368 (7th Cir. 1984), the court reaffirmed the use of the federal larceny statute, 18 U.S.C. § 641, for the theft of personal services. Id.
4. Computer Data and Programs as “Property”

Most computer-related crimes are, in essence, offenses against intangible property, such as computer data or programs. These crimes are difficult to prosecute under traditional statutes because “property” is often defined only as real or personal property. The Computer Fraud and Abuse Act circumvents this problem by making the act of unauthorized access the criminal offense. In effect, however, the Act creates a right of protection for specified kinds of information. This approach could result in an increasing miscellany of new statutes, each aimed at protecting a specified class of information. Rather than enacting more computer crime laws to protect specified information, criminal law could be simplified by including certain forms of intangible property within the definition of property in existing statutes.

Several states have already amended their theft statutes to include intangible property. Recently in Virginia, the Supreme court in Evans v. Commonwealth affirmed an embezzlement conviction for the theft of stored data. At the federal level, information contained in government computer files has been held to be within the definition of property in the larceny statute. In United States v. Girard, the defendants copied and subsequently sold information contained in the computer files of the Drug Enforcement Agency. Finding a property interest in the content of private records, the court stated that the definition of larceny included the “misuse or abuse of property” or its use “in an unauthorized manner,” and affirmed the defendants’ convictions.

In a concurring opinion, Justice Dumbauld argued that the statutory expansion should have been accomplished through legislative efforts. See supra note 4, at 9. See, e.g., W. VA. CODE § 2-2-10(q) which defines “personal property” as including “goods, chattels, real and personal, money, credits, investments and the evidences thereof.” Id.

180. House Report, supra note 4, at 9. See, e.g., W. VA. CODE § 2-2-10(q) which defines “personal property” as including “goods, chattels, real and personal, money, credits, investments and the evidences thereof.” Id.

181. At present, coverage under the Act extends to financial, credit, and government owned information. 18 U.S.C.A. § 1030(a)(1)-(3) (West Supp. 1985). The 99th Congress is presently considering a computer crime bill penalizing unauthorized access to medical records. See supra note 17 and accompanying text.

182. The 99th Congress is presently considering a computer crime bill penalizing unauthorized access to medical records. See supra note 17 and accompanying text.

183. Professor Raymond August argues that defining property to include intangible property would both simplify the theory of criminal law and free the courts to focus on the injury to the victim. August, Turning the Computer Into a Criminal, 10 BARRISTER 12, 15 (1983). The Model Penal Code has included intangible property in its definition of property. MODEL PENAL CODE AND COMMENTARIES § 225.0(6) (Official Draft and Revised Comments 1980).

184. See, e.g., MASS. GEN. LAWS ANN., ch. 266, § 30 (West 1985); VA. CODE § 18.2-98.1 (1982). The Virginia statute provides that “[c]omputer time or services or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny . . . .” Id.


187. Id.

188. Id. at 70.

189. Id. at 71.

190. Id. at 73.
5. Prosecuting Computer-Related Crime Under U.S. Laws

For crimes involving computers, it appears that a conviction is not dependent only on the adequacy of existing laws, but on the prosecutor's proper classification of the crime. Prosecution under the Computer Fraud and Abuse Act is based on the premise that computer use itself, for specific unauthorized or criminal purposes, should be a criminal activity. In most cases, however, prosecution based on the results of the computer-related activity, such as fraud or theft, is more appropriate.

For example, in a hypothetical computer-related crime, the defendant, without authorization, uses a government-owned account password to access a private university computer for his own use. The U.S. government is subsequently billed for the computer time that the defendant used. For the prosecutors, the choice of an applicable statute depends on their characterization of the crime.

If the prosecution characterizes the crime as a theft of government-owned property, they could seek a conviction under the federal larceny statute, for conversion of the account password. At least one court has held that information in computer files is a "thing of value" under the statute. It is reasonable to assume that a court would also find that an account password, stored within the computer, is information.

Alternatively, prosecutors could proceed under the Computer Fraud and Abuse Act, based not on the unlawful conversion, but on unauthorized access to information in a government computer. While prosecution under the federal larceny statute goes to the nature of the underlying crime, prosecution under the Computer Fraud and Abuse Act depends on whether a government computer is involved.

If the account password had been taken from a computer other than a government computer, there would be no basis for prosecution under the Computer Fraud and Abuse Act. Earlier versions of the Computer Fraud and Abuse Act did contain provisions which included unauthorized access to any public or private computer system. As enacted, however, the Computer Fraud and Abuse Act covers only unauthorized access to computers operated by the federal government and by financial institutions. More specific federal crimi-

191. These facts are adapted from the Canadian case of Regina v. Marine Resource Analysts. See supra text accompanying notes 53-59.
195. In Marine Resource Analysts, the defendant was found guilty of fraud, not unauthorized access. See supra notes 53-59 and accompanying text.
196. See supra text accompanying notes 129-34.
nal legislation could be enacted to protect private computer systems. An alternative to penal sanctions, however, may provide a more comprehensive model for preventing all computer-related crime.

IV. PREVENTING COMPUTER-RELATED CRIME

"Laws act after crimes have been committed; prevention goes before them both." — J.G. Zimmerman

A major objective of the Computer Fraud and Abuse Act was to discourage incidents of external access by hackers to government computers. A large proportion of computer-related crime, however, is perpetrated by inside employees with easy access to a computer. The inadequacy or nonexistence of internal security controls for computer systems only enhances the opportunities to commit computer-related crime. Although criminal legislation can deter crime to some extent through the creation of sanctions, its efficacy is decreased when, in effect, the safe is left unlocked.

The Small Business Computer Security and Education Act of 1984 (Computer Security and Education Act) was enacted to improve the management of information technology within small businesses, and to educate and encourage those businesses in the use of computer security techniques. The Act focuses on the prevention of computer-related crime through the protection of information.

The major provision of the Act establishes a Computer Security and Education Advisory Council whose function is to advise the Small Business Administration on the nature and scope of computer crime, the effectiveness of state and federal legislation on deterrence and prosecution, the effectiveness of management techniques to improve computer security, and the development of guide-

199. See supra note 108 and accompanying text.
203. Small businesses are particularly vulnerable to computer-related crimes because they have fewer resources available for system security or security audits. 130 Cong. Rec. S6522 (daily ed. May 24, 1984).
205. Id. at 7-9. The Report cites Sanford Sherizen's "rules of business" for the computer age:
   1) Computer security is no longer an optional decision but may be fundamental to the survival of a business; 2) The core issues of computer security can and must be understood by nontechnical managers; 3) The essence of computer security lies with management controls, reviews and policies developed with the active support and involvement of top management; and 4) There are a variety of management questions which can be raised with technical staffs in order to evaluate the adequacy of computer protections in business.
Id. at 7.
lines for evaluating system security.\textsuperscript{207} The Small Business Administration, in
turn, disseminates this information to small businesses through forums and
training sessions.\textsuperscript{208}

Although the Computer Security and Education Act focuses on protection for
small businesses, the issues addressed in the Act are also relevant to large
businesses and government.\textsuperscript{209} Many computer-related crimes, even when dis-
covered, may go unreported for fear of loss of business reputation or public
confidence.\textsuperscript{210} This only emphasizes the need to improve computer system secu-
rity to effectively prevent computer-related crime.

Education in computer security techniques also facilitates the investigation of
computer-related crimes. Since 1976, the FBI has run training courses which
familiarize students with computer operations and programming.\textsuperscript{211} As part of
this training, students access a data base of simulated financial records, identify-
ing the methods of obtaining money through a computer.\textsuperscript{212} In California,
private computer industry experts lead similar training programs for local law
enforcement officials.\textsuperscript{213} These efforts should be encouraged to improve the
detection and prevention of computer-related crimes.

V. ANALYSIS AND CONCLUSION

Before enacting more computer crime laws, legislators should evaluate the
interplay between the importance of computer system security and the status of
information within the definition of property. The new Computer Fraud and
Abuse Act, for example, makes it a crime to enter the computer/"safe" when it is
still unclear whether the information/"goods" can be stolen.

The categorization of computer information as a "thing of value" under the
U.S. larceny statute\textsuperscript{214} should serve as a prototype for the prosecution of theft of
computer data and programs. This approach was followed by the Ontario Court
of Appeal in the Canadian case of Regina v. Stewart,\textsuperscript{215} which held that confiden-

\begin{footnotesize}
\begin{enumerate}
\item 209. For example, the General Accounting Office recently published a report criticizing the lack of
    security in federal computer systems. General Accounting Office, Federal Information Systems
    Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, Masad-
    82-18 (April 21, 1982).
\item 210. See Sokolik, supra note 2, at 359. This is particularly true for financial institutions. See also
    Hearing on H.R. 3970, supra note 14, at 72.
\item 211. Hearings on 3970, supra note 23, at 9.
\item 212. Id. See also Crim. Just. Newsletter, Apr. 25, 1983, at 6 col. 1 [hereinafter cited as Newsletter].
\item 213. This project is a joint effort of the local law enforcement agencies, the California Department of
    Justice, and the FBI. Newsletter, supra note 132b. The computer crime unit is headed by District
    Attorney Leo Himmelsbach of Santa Clara County, California. Id.
\item 214. See supra text accompanying notes 186-90.
\item 215. 42 Ont. 2d 225 (1983).
\end{enumerate}
\end{footnotesize}
tial information stored in a computer was subject to theft. The Stewart court specifically rejected the English case *Oxford v. Moss*, and instead cited with approval several U.S. cases holding that information was within the definition of property.

In England, the seemingly contrary holding in *Oxford v. Moss* need not preclude application of the Theft Act to theft of computer information. *Oxford v. Moss* could be interpreted as indicating that the memorization of information, in itself, does not constitute theft. Such an interpretation would be consistent with both Canadian and U.S. cases, and allow for the prosecution of theft of computer information without resort to specific computer crime legislation.

Canada has also extended its interpretation of information as property to crimes involving the alteration of computer data. In *Turner and the Queen*, this was accomplished through the use of the mischief statute, which prohibits interference with the use of property. In England, the questionable status of information as property might preclude prosecution of the alteration of computer data. The Theft Act, however, has been applied to schemes involving the alteration of data where the underlying crime resulted in a fraud or theft.

In the United States, the federal mischief statute, requires a physical depre-
dation against property. This requirement effectively prevents federal pro-
secutors from using the mischief statute to prosecute for alteration of informa-
ton in computer files. If the Canadian approach is adopted in the United States, the federal mischief statute should be amended to include any interference with government property. As with the U.S. federal larceny statute, prosecutors

216. Id. at 240.
218. 42 Ont. 2d at 239, 241-42.
219. 68 Crim. App. 183 (1979). The *Oxford* court held that confidential information was not within the definition of property for purposes of the Theft Act 1968. See supra text accompanying notes 84-86.
221. See supra note 74.
222. See supra text accompanying notes 90-98.
223. 18 U.S.C. § 1361 (1982). The statute provides:

> Whoever willfully injures or commits any depredation against any property of the United States, or any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, shall be punished as follows:

> If the damage to such property exceeds the sum of $100, by a fine of not more than $10,000 or imprisonment for not more than ten years, or both; if the damage to such property does not exceed the sum of $100, by a fine of not more than $1,000 or by imprisonment for not more than one year, or both.

*Id.*

224. The court in United States v. Jenkins defined depredation as the acts of plundering, robbing or pillaging. 554 F.2d 783 (6th Cir. 1977).
225. See supra note 74. Alternatively, federal legislators could adopt the approach of the Washington state mischief statute which in relevant part, provides:

> "Physical damage", in addition to its ordinary meaning, shall include the total or partial alteration, damage, obliteration, or erasure of records, information, data, computer programs,
would have the choice of using either the new mischief offense or an applicable provision of the Computer Fraud and Abuse Act.

The classification of computer services as property has allowed for successful prosecution of the theft of computer time or services. This approach is best exemplified by recent interpretations of the U.S. federal larceny statute which have construed services as a thing of value.\textsuperscript{226} Criminal statutes which specifically prohibit the theft of services, as in section 1 of the English Theft Act 1978,\textsuperscript{227} are often inapplicable to computer services due to requirements that the services be provided in expectation of payment.\textsuperscript{228} For prosecution of this crime in the United States, the expanded use of larceny statutes may be the only method available, because the Computer Fraud and Abuse Act exempts the theft of computer time from coverage.

In the United States, the relationship between information and property often varies, depending primarily on an individual court's interpretations of property in a given criminal statute. At the federal level, the Computer Fraud and Abuse Act, in effect, creates a "property right" in owners of certain classified information and financial data. The proliferation of criminal laws based on subject matter of information may be the unwelcome result of such an approach. This may already be occurring at the state level, where computer crime legislation now exists in thirty-five states.\textsuperscript{229} Over half of these laws were either enacted or amended during 1984 alone.\textsuperscript{230}

or their computer representations, which are recorded for use in computers or the impairment, interruption, or interference with the use of such records, information, data, or computer programs, or the impairment, interruption, or interference with the use of any computer or services provided by computers.

\textsuperscript{226} See supra text accompanying notes 172-74.
\textsuperscript{227} See supra note 100.
\textsuperscript{228} See infra text accompanying notes 99-104, 163-66.

\textsuperscript{230} Supra note 229.
For the United States, Canada, and England, a viable alternative to the enactment of computer crime statutes is the expansion of the definition of property within offenses to include intangible property, such as computer data. Clearly, more effective deterrence of computer-related crime requires a more uniform treatment of information as an asset under existing laws. Both the private sector and the legislature must work together, however, to insure that information receives the most effective protection possible.

Lisa Menelly