Pace International Law Review

Volume 3 | Issue 1 Article 8

1-1-1991

Computer Hacking: A Global Offense

Robert J. Sciglimpaglia, Jr.

COMMENTS

COMPUTER HACKING: A GLOBAL OFFENSE

INTRODUCTION

INTRODUCTION

On March 19, 1990 a program written by three hackers[1] entered dozens of computers hooked to Internet, an international

---

[1] Generally, a hacker is a person who illegally and without authorization gains access to a computer system. *See generally* Cangialosi, *The Electronic Underground: Computer Piracy and Electronic Bulletin Boards*, 15 RUTGERS COMPUTER & TECH. L.J. 265 (1989).

A hacker also has been defined as "a person who enjoys learning the details of computer systems and how to stretch their capabilities," and "one who programs enthusiastically." Bloombecker, *Computer Crime Update: The View as We Exit 1984*, 7 W. NEW ENG. L. REV. 627, 629 n.2 (1985) (quoting STEELE, WOODS, FINKEL, CRISPIN, STALLMAN, & GOODFELLOW, THE HACKER'S DICTIONARY 79-80 (1984).

Additionally, a hacker has been described as a "cracker" who breaks into high security computer systems for fun and to look around. Cangialosi, *supra*, at 269-70.

A hacker is also "a person who is not trying to learn about computers in a meaningful manner, but rather by trial and error." WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 168 (3d. ed. 1988) [hereinafter COMPUTER DICTIONARY].

Although no universal definition of a hacker exists, a hacker has been described as a male, usually juvenile, and almost always under the age of 25. A hacker is relatively intelligent, shy, and quiet. Relatively few females have been caught hacking, one exception is Susan Headley, also known as "Susan Thunder." Bloombecker, *supra*, at 630-631, n.12.

Once in the system the hacker may browse, change or delete files, disable the system

network.[2] The program stole electronic documents containing users' passwords and erased files to keep itself undetected.[3]

On April 2, 1990, three Australians were arrested on charges of tampering with Internet computers linked in the United States and Australia.[4] Australian Federal Police made the arrests as a result of an investigation initiated in 1988 in cooperation with United States authorities.[5]

Computer specialists are disturbed because the hacking in-

---

by introducing a program such as a virus, or steal funds or other goods by electronic transfer. *See generally* Schulkins, *The Electronic Burglar*, 1 COMPUTER L. & PRAC. 140 (1985); Cangialosi, *supra*; Soma, Smith and Sprague, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571 (1985) [hereinafter Soma].

Hacking also includes computer aided abuse, theft of computer time, or software piracy. Computer aided abuse includes theft of money or other property by means of a computer. *See* Becker, *Rifkin: A Documentary History*, 2 COMPUTER/L.J. 471 (1980); PREVENTION COMMITTEE, PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICACY, COMPUTERS: CRIMES, CLUES AND CONTROLS 10 (1986) [hereinafter PREVENTION COMMITTEE].

An example of theft of computer time is when an employee uses a company computer to store personal data. *See* A. BEQUAI, HOW TO PREVENT COMPUTER CRIME 20 (1983).

Software piracy is the illegal copying of computer programs for sale or personal use. This concerns the copyright aspects of computer crime. *See* Brown, *International Trends in Computer Program Protection*, 3 COMPUTER L. & PRAC. 157 (1987).

Computer hacking is characterized as a computer crime, as well as a white-collar crime. *See generally* L. SIEGAL, CRIMINOLOGY 369-71 (2d. ed. 1986). Siegal defines white-collar crime as "the illegal activities of people and institutions whose acknowledged purpose is profit and gain through legitimate business transactions." *Id.* at 367. This definition would encompass thefts of money by computerized transfers, computer time (i.e., Lexis and Westlaw), and computer data. *See* Note, *Who is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 92 (1985) (authored by Diana Smith).

White-collar crime has also been defined as "any illegal act characterized by deceit and concealment and not dependent on the direct application of physical force." A. BEQUAI, COMPUTER CRIME 1 (1976). [hereinafter COMPUTER CRIME]. This definition would encompass the unauthorized access component of hacking because the hacker does not physically confront his victims; he gains illegal access via telephone lines. *See also* D. PARKER, CRIME BY COMPUTER (1976).

[2] Markoff, *Computer System Intruder Plucks Passwords and Avoids Detection*, N.Y. Times, Mar. 19, 1990, at A12, col. 4 [hereinafter *Password Plucker*].

Among the institutions penetrated were the Los Alamos National Laboratory, Harvard University, the Digital Equipment Corporation, Lawrence Livermore National Laboratories, Boston University, New York University, the University of Texas and Belicore, a telephone research laboratory. Markoff, *Arrests in Computer Break-Ins Show a Global Peril*, N.Y. Times, Apr. 4, 1990, at A1, col. 2 [hereinafter *Global Peril*].

See infra note 21, for definition of a network.

[3] *Password Plucker*, *supra* note 2.

[4] *Global Peril*, *supra* note 2.

[5] *Id.*

cident raises "troubling questions about the vulnerability of technology to intruders operating beyond American borders and laws."[6] "Any computer that is connected to a telephone or any computer that is connected to a computer network is vulnerable. It doesn't matter what continent they are on."[7]

The Australian Federal Police said that while they knew about the illegal hacking activities since 1988, they could not begin their investigation until July, 1989 when legislation covering computer crimes became effective in Australia.[8] Under the statute, it is a crime to break into computer systems located anywhere in the world from telephones or computer links originating in Australia.[9]

The police maintain the hackers spent up to sixteen hours per day for approximately two years perfecting their craft of illegally entering computers.[10] One of the hackers even boasted to The New York Times, in an anonymous telephone call, that he had broken into Internet in order to taunt security specialists who denounced such activities.[11] Although security experts generally deplore the act of hacking, one benefit that arose from the Australian incident is that the break-ins uncovered previously unknown security flaws in the computer systems.[12]

---

[6] *Id.*

[7] *Id.* This statement was made by Peter Neumann, a computer scientist at SRI International, a research center in Menlo Park, California. *Id.*

[8] *Id.* at A16. At the time this Article went to press, another international hacking incident presented itself illustrating the dilemma when countries do not have anti-hacking statutes. The New York Times reported on April 21, 1991 that a group of Dutch hackers had been breaking into United States military computers for almost six months. The computers penetrated were all linked to the Internet network, as with the Australian incident. Markoff, *Dutch Computer Rogues Infiltrate American Systems With Impunity*, N.Y. Times, Apr. 21, 1991, at A1, col. 5 [hereinafter *Dutch Rogues*]. The hackers actions did not cause serious damage and no arrests were made because there are no legal restrictions in the Netherlands barring hacking. *Id.*

[9] *Id.* at A1.

[10] *Global Peril*, *supra* note 2, at A16.

[11] *Id. See also* C. STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE 354 (1990).

[12] *Global Peril*, *supra* note 2, at A16. Uncovering of security flaws in computer systems has sparked a debate over whether hackers should be considered criminals. In *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing* by Tom Forester and Perry Morrison, a section is entitled "Hackers: Criminals or Modern-Day Robin Hoods?" The authors argue that hackers should not be treated as criminals for exposing security flaws in systems required to be secure (for example data bases which contain personal information on individuals). The authors also offer that the Chaos Computer

The Australian hacking incident illustrates not only the vulnerability of computer security, but also serves as a prototype representing an entire hacking phenomenon. The hacking incident also demonstrates the need for international measures and legislation—both domestic and international—aimed at punishing, and perhaps preventing, global hacking.[13]

The Australian hacking incident further is demonstrative of a large-scale problem arising from the failure of legal systems to keep pace with rapid advancements in technology. Aside from the issue of hacking, it has been reported that facsimile machines, commonly known as fax machines, have been hacked from around the globe.[14]

Section I of this Comment defines hacking and discusses how it is accomplished. Section II analyzes international legal problems and approaches associated with global hacking. Section III discusses the two approaches used in domestic law. Sections IV through VI offer specific analysis of legal measures ad-

---

Club, a hacker group, released more information about the USSR Chernobyl nuclear disaster than did the West German government. FORESTER & MORRISON, COMPUTER ETHICS: CAUTIONARY TALES AND ETHICAL DILEMMAS IN COMPUTING 49-50 (1990). *See also* Schwartz, *Hackers of the World Unite*, NEWSWEEK, July 2, 1990, at 36.

[13] This Australian incident is not the first time hacking has crossed international borders. In Regina v. Turner, 27 B.L.R. 207 (1984, Ont. H.C.) *aff'd* Ont C.A. (February 14, 1985) *cited in* MANN, COMPUTER TECHNOLOGY AND THE LAW IN CANADA 171 (1987), hackers accessed a Milwaukee Corporation's computer from Toronto and disabled it so the Corporation could not access any data stored in the system.

Also, a group called the Chaos Computer Club of Hamburg, West Germany was able to access 135 computer systems worldwide, extracting information about the space shuttle, Strategic Defense Initiative (Star Wars), and other NASA projects. Marbuck, *Hacking Through NASA: A Threat or Only an Embarrassment*, NEWSWEEK, Sept. 28, 1987, at 38; Cangialosi, *supra*, note 1, at 270.

[14] Cullison, *Fax Machines Become an Open Book To Hackers' Prying Eyes*, Chicago Tribune, Sept. 9, 1990 at 11C [hereinafter *Prying Eyes*]; Cullison, *Warning: 'Fax Hackers' Can Silently Steal Your Business Messages*, The Stamford Advocate, Sept. 9, 1990, at E1, col. 1; Hillkirk, *The Fax of the Matter: It Can Be Intercepted*, USA Today, October 19, 1989, at B1.

> [A]nyone with a little knowledge of electronics can tap fax messages being sent from one of these relatively unsophisticated machines to another, with the duplication printed out on the pirate's facsimile machine. Both the sender and the receiver of the faxed document remain completely unaware that they have been bugged.

Prying Eyes, *supra*, at 11C.

The facsimile hacking phenomenon is beyond the scope of this article, however, the issues of facsimile and computer hacking are essentially similar and both need to be addressed on a global scale.

dressing hacking in Canada, the United States and the United Kingdom. Finally, Section VII offers potential solutions to the hacking crisis.

I. THE PROCESS OF COMPUTER HACKING

A. *Finding and Penetrating Computer Systems*

Basically, there are two types of computer systems: "closed" and "remote."[15] A "closed" system has separate terminals.[16] These terminals are directly "hard-wired"[17] to a central mainframe computer[18] located in the same facility as the terminals. The "closed" system cannot be accessed[19] from outside computers, thus neither authorized nor unauthorized outside users can "log on."[20]

---

[15] These terms are the author's generalization for this article. *See generally* R. WALKER, UNDERSTANDING COMPUTER SCIENCE-VOL. II (1985); A. BEQUAI, HOW TO PREVENT COMPUTER CRIME (1983) [hereinafter PREVENTION].

[16] A terminal is "[a] keyboard/display of keyboard/printer device used to input programs and data to the computer and to receive output from the computer." COMPUTER DICTIONARY, *supra* note 1, at 378.

There are two types of terminals: a smart terminal and a dumb terminal. A smart terminal is "[a] terminal that contains some capacity to process information being transmitted or received." *Id.* at 348.

A dumb terminal is "[a] visual display terminal with minimal input/output capabilities and no processing capabilities." *Id.* at 121.

[17] "Hard wired" means a "physical connection of two pieces of electronic equipment by means of a cable" or wire. *Id.* at 170.

[18] A mainframe computer is:

> A large, expensive computer generally used for information processing in large businesses, colleges, and organizations. Originally, the phrase referred to the extensive array of large rack and panel cabinets that held thousands of vacuum tubes in early computers. Mainframes can occupy an entire room and have very large data-handling capacities. They are far more costly than microcomputers or minicomputers. Mainframes are the largest, fastest and most expensive class of computers. (Supercomputers are the largest, fastest and most expensive of the mainframes).

Id. at 225.

[19] For outside access, the mainframe must be equipped with a modem. A modem is basically a device that enables computers to communicate with each other. A modem is "[a]n acronym for MOdulator/DEModulator, a device that translates digital pulses from a computer into analog signals for telephone transmission, and analog signals from the telephone into digital pulses the computer can understand. The modem provides communication capabilities between computer equipment over common telephone facilities." *Id.* at 241.

[20] To be "Logged on" a computer basically means to have accessed the computer via a terminal. Logging in is "[t]he process of establishing communication with and verifying

Similar to the "closed" system, the "remote" system also has terminals that may be hard-wired to the mainframe. But what distinguishes the "closed" and "remote" systems is the "remote" system's capability to be linked[21] with computers outside the facility.[22] Basically, this connection is accomplished when the outside computer sends a signal by modem[23] to the "remote" system.

Of the two systems, the "remote" is more common because the "remote" can perform business functions such as: electronic fund transfers;[24] electronic mail;[25] providing up-to-date information on stock quotes;[26] and office work can be done at home.[27]

---

the authority to use the computer during conversational programming." *Id.* at 214.

In rare cases, the information from these closed systems can be assessed by unauthorized users through the use of an electromagnetic pickup. These pickups intercept radiation generated by the closed computer and converts that radiation into readable data which another computer system can understand. This detection can not be accomplished through phone lines. PREVENTION, *supra* note 15, at 23.

[21] A link is "[i]n data communications, a physical connection between one location and another whose function is to transmit data." *Id.* at 211.

A link is usually achieved through the use of telephone lines and networks. A network is "(1) A system of interconnected computer systems and terminals. (2) A series of points connected by communications channels. (3) The structure of relationships among a project's activities, tasks and events." *Id.* at 253.

See also INTERNATIONAL BUSINESS MACHINES CORP., COMMUNICATION SYSTEMS CONCEPTS (1977); W. BARDEN, JR., NETWORK PRIMER (1986); G. FRIEND, J. FIKE, H. BAKER, & J. BELLAMY, UNDERSTANDING DATA COMMUNICATIONS (1984) [hereinafter FRIEND]; WANG LABORATORIES, INC., THE WANG PROFESSIONAL COMPUTER: NETWORK USER GUIDE (2d ed. 1984); A. TANENBAUM, COMPUTER NETWORKS (1981).

[22] Most often, personal computers are used to link to computers from outside of its facility. A personal computer is "[a] moderately priced microcomputer system intended for personal use rather than commercial purposes." COMPUTER DICTIONARY, *supra* note 1, at 279.

[23] *See supra* note 19 for definition of "modem."

[24] Electronic fund transfers (EFT) are "[a] cashless method of paying for goods or services. Electronic signals between computers are used to adjust the accounts of the parties involved in a transaction." COMPUTER DICTIONARY, *supra* note 1, at 128. An example of an EFT is direct deposit of a paycheck to an employee's bank account.

[25] Electronic mail is "[t]he process of sending, receiving, storing, and forwarding messages in digital form over telecommunication facilities." *Id.* at 128.

See also COMPUSERVE INC., COMPUSERVE INFORMATION SERVICE: USERS GUIDE § 4 (1986) [hereinafter USERS GUIDE]; C. BOWEN & D. PEYTON, HOW TO GET THE MOST OUT OF COMPUSERVE 42-47 (3d ed. 1987).

[26] Corporations can check a particular stock quote through services such as CompuServe. *See* USERS GUIDE, *supra* note 25, at § 7; BOWEN & PEYTON, *supra* note 25, at 285-91.

[27] To work from home, an employee needs a computer and a modem to access the business system and a password. *See supra* note 19 and accompanying text.

Furthermore, "remote" systems also are used internationally by governments to send information to other countries. Such information can include data pertaining to air transport control or meteorological weather.[28]

B. *The Complexities Behind Detection and Prosecution*

As evidenced by the recent hacking arrests in Australia, hacking is a time-consuming process.[29] Because it takes considerable time for hackers to penetrate a system, the owners of the system are lulled into a false belief that their system is secure.[30] The considerable time element involved in hacking a system might also foster a misconception that hackers are easily traceable because they continuously dial a telephone number and attempt to achieve access.[31] An explanation of how hacking is accomplished will further illustrate why these beliefs are false.

The initial step in accessing a remote system is for a hacker to discover the system's telephone number. Knowledge of the system's telephone number is achieved by using a program called a "random number generator"[32] or by manually dialing random numbers until a computer system is contacted. Hackers also obtain telephone numbers from Bulletin Board Services (BBS).[33]

Second, after obtaining a viable telephone number, the

---

[28] INSTITUTE FOR RESEARCH ON PUBLIC POLICY, ISSUES IN CANADIAN/U.S. TRANSBORDER COMPUTER DATA FLOWS 40 (W.E. Cundiff & M. Reid ed. 1979).

[29] *See supra* note 10 and accompanying text.

[30] *See generally* FORESTER & MORRISON, *supra* note 12, at 40-67; COMPUTER CRIME, *supra* note 1, at 13; J. CARROLL, COMPUTER SECURITY 251 (1977).

[31] *See supra* text accompanying note 10 as an example of the time element.

[32] A random number generator is either written by a hacker or purchased. A random number generator is "[a] computer program or hardware designed to produce a pseudo random number or series of pseudo random numbers according to specified limitations." COMPUTER DICTIONARY, *supra* note 1, at 310.

[33] These BBS hacker boards are widespread. *See* SOMA, *supra* note 17; Cangiolosi, *supra* note 1.

The BBS is a public or private service used to exchange messages or software and is set up and run by a systems operator or SYSOP. The BBS is "[a] computer system that allows users to post messages or programs for other users." COMPUTER DICTIONARY, *supra* note 1, at 36.

An example of a large commercial BBS is CompuServe, but there are also many small, private services available. Estimates say there are approximately 3500-4500 private services. Cangiolosi, *supra* note 1, at 266.

hacker must connect his modem with the modem of the system being accessed. During the connection process, time-consuming errors may cause the hacker to have to backtrack to re-entering the system's telephone number.[34]

After the modems finally connect, the hacker's third task is to discover a password or user code[35] of an authorized user. Again, this is an additional time-consuming step because secure computer systems have multiple-level passwords and often automatically terminate the phone/modem connection[36] after a designated number of incorrect passwords have been entered.[37]

The hacking problem is compounded because many countries do not have laws addressing the phenomenon.[38] This lack of legal protection leads hackers to believe they will escape prosecution and thus are not deterred from their intrusive activi-

---

[34] Errors occur when information is transmitted via telephone lines and the errors prohibit the transfer of understandable information. FRIEND, *supra* note 21, at 5-4.

Errors occur if the "protocols" or "parameters", as well as other variables, of the system the hacker is attempting to access are not matched with his own system.

Protocols are a "[s]et of rules or conventions governing the exchange of information between computer systems." COMPUTER DICTIONARY, *supra* note 1, at 304.

Parameters are "[a]n arbitrary constant. A variable in an algebraic expression that temporarily assumes the properties of a constant." *Id.* at 273. Examples of parameters are stop bits, baud rate, etc. *See* BOWEN & PAYTON, *supra* note 25, at 18.

[35] The password or user code, is the secret, special word, code, or symbol that must be presented to the computer system to gain access to its resources. It is used for identification and security purposes on a computer system. Each user is assigned a specific set of alphanumeric characters to gain entrance to the entire computer system or to parts of the system.

COMPUTER DICTIONARY, *supra* note 1, at 276.

The hacker, in order to access the system must use an authorized user's password or user code. Use of this code by the hacker can prevent the authorized user from gaining access to the system. *See generally* Schulkins, *supra* note 1.

Similar to the random number generator, a random character generator program can be purchased or written by a hacker. The latter program enters letters and numbers in an attempt to discern the user's access code. *See supra* note 34 and accompanying text.

[36] If the telephone/modem connection is terminated, the hacker must re-dial the telephone number and enter a different access code. Statutes in some countries and within the United States criminalize telephone harassment. These statutes have been used to prosecute hacking offenses. These statutes typically prevent repeated re-dialing of a telephone number if no legitimate purpose of communication is intended, whether or not conversation occurs. Soma, *supra* note 1, at 575.

[37] Schulkins, *supra* note 1, at 140.

[38] *See generally* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 10 COMPUTER RELATED CRIME: ANALYSIS OF LEGAL POLICY (1986) [hereinafter OECD].

ties.[39] Fortunately for the Internet computer users in the United States, Australia's statute enabled the perpetrators to be brought to justice.[40]

Even when hacking victims are fortunate enough to have a remedy via statute, prosecution of hacking offenses may still be problematic. First, many hackers are juveniles and thus are immune from prosecution.[41] Second, detecting some hacking offenses is difficult and sometimes impossible.[42] Finally, a reluctance frequently exists on the part of victims of hacking to report the crime.[43]

---

[39] Hackers believe that they will not be subject to prosecution. This is evidenced from the statement of the Australian hacker who said he did not believe he was chargeable with a felony for his actions. *Global Peril*, *supra* note 2, at A16. This belief by hackers may be justified if they hack from nations without specific anti-hacking legislation as evidenced from the most recent Dutch incident. *See Dutch Rogues*, *supra* note 8.

[40] *Global Peril*, *supra* note 2, at A16. Unfortunately for the United States Internet users however, the Netherlands does not have an anti-hacking statute under which the Dutch hackers can be brought to justice. Thus, they are hacking with impunity. *Dutch Rogues*, *supra* note 8.

[41] Bloombecker, *supra* note 1, at 640. Some have advocated punishment of these juveniles by confiscating their computer equipment, or by penalizing their parents through tort or criminal liability for not adequately supervising their children's hacking activities with the computer which the parents probably purchased. *Id.* at 636. *See also* Soma, *supra* note 1, at 576-77.

[42] One reason why detection is often hindered is that the hacker will use a valid password to access the system thus, it will appear as if an authorized user logged on. PREVENTION, *supra* note 15, at 22. Also, as illustrated by the Australian case, a clever hacker can create a program to conceal his unauthorized access. *Password Plucker*, *supra* note 2, at A12.

[43] Reluctance to report can be attributed to the fact that harm was minimal, embarrassment that a security lapse existed or fear of a repeat situation by "copy-cats" who heard of the incident through the media and believe the target to be easy. H.R. Rep. No. 894, 98th Cong., 2d Sess. 11, *reprinted in* 1984 U.S. CONG. & ADMIN. NEWS 3689, 3697.

Reported computer crime has been referred to as "the tip of the iceberg." Schulkins, *supra* note 1, at 140. This is evidenced by the 1984 survey conducted by the American Bar Association's Criminal Justice Section Task Force On Computer Crime. MANN, COMPUTER TECHNOLOGY AND THE LAW IN CANADA 156 (1987) (citing Task Force on Computer Crime, *Report on Computer Crime* (American Bar Association, June, 1984)). The survey was distributed to 1,000 of the United States largest corporations and government agencies. Of the 1,000, only 283 responded. Of the respondents, twenty five percent acknowledged a known and verifiable loss due to computer crime in the preceding twelve months. The twenty five percent figure is computed from seventy-two of the 275 who responded to that particular question. *Id.* Of those twenty five percent, the majority had suffered losses in the range up to $100,000. Wasik, *Surveying Computer Crime*, 1 COMPUTER L. & PRAC. 110, 111 (1985). Eighteen cases reported higher losses. *Id.* And one case reported a loss between $100 million and $500 million. *Id.*

However, only about one-third of those who were victims of computer crime in this

II. INTERNATIONAL PRINCIPLES APPLYING TO HACKING OFFENSES

A. *The Non-Presence of a Hacker*

Computer hacking is a crime unlike any other under international law. Under a normal scenario, a person commits a criminal act in the country where he is physically present. For example, if A were to commit a bank robbery in Country X, he would have to be in X to commit the offense. This would mean that Country X would have jurisdiction in investigating A's crime and bringing A to trial in state X, or it could return A to his home country.[44]

Hacking is a unique offense in that A may commit a bank robbery by computer in Country X while he is physically present in his home, Country Y. The bank robbery could be accomplished if the hacker illegally accessed a bank in Country X and transferred funds from an account in Country X's bank into his own bank in Country Y. This presents an immediate problem to Country X in obtaining jurisdiction over A and in investigating his crime.[45] The following sections discuss the status of the individual under international law, extradition, the double criminality standard, and treaties on mutual assistance.

B. *International Law and the Individual*

Historically, sovereign states, rather than individuals, were the main subject of international law.[46] Since World War II, however, the individual is properly considered subject to the ju-

---

survey had reported the crime to law enforcement authorities. *Id.*

In other statistics, it has been estimated that only one in 100 computer crimes are detected, only one in five that are detected are reported, and only one in 100 are prosecuted. MANN, *supra* at 157.

[44] INTERNATIONAL CRIMINAL LAW: A GUIDE TO U.S. PRACTICE AND PROCEDURE 335-341 (V. Nanda & M. Bassiouni ed. 1987). The returning of an individual to his native country ensues only when an extradition treaty exists between the native country and the nation where a crime is allegedly committed. *Id.* at 339.

[45] *See supra* text accompanying note 5 where the United States had to rely upon Australian police to investigate the crime.

[46] 1 A TREATISE ON INTERNATIONAL CRIMINAL LAW 104 (Bassiouni & Nanda ed. 1973) [hereinafter TREATISE].

Jessup writes, "international law or the law of nations must be defined as law applicable to states in their mutual relations and to individuals in their relations with states." JESSUP, A MODERN LAW OF NATIONS 17-18 (1948) *quoted in* HENKIN, PUGH, SCHACHTER & SMIT, INTERNATIONAL LAW: CASES AND MATERIALS 352 (2d ed. 1987) [hereinafter HENKIN].

risdiction of international law.[47] Hence, an individual can be deemed to be in violation of international law, regardless of whether punishment is rendered by the states, individually, or by international courts.[48] However, in order for an individual to be liable under international law, the person must commit an offense defined under customary international principles, be they norms or treaties.[49]

Hacking poses a problem in the international community because there is no customary principle outlawing it.[50] Because the offense is relatively new, no international norms exists concerning hacking and there are no treaties, conventions or United Nations Resolutions directly pertaining to the computer crime.[51] As a result, hacking offenses must be attacked solely through domestic legislation. Thus, an individual cannot be subject to international sanctions as a result of hacking; for domestic remedies are all that is available. Consequently, tensions exist in obtaining cooperation among states to ensure that domestic anti-hacking statutes are enforced.

C. *Extradition Treaties, Double Criminality and the Hacker*

One such tension spurs from extradition treaties. Such treaties provide the legal arrangement between party states for bringing an alleged criminal within the jurisdiction of the court

---

[47] TREATISE, *supra* note 46, at 104-05. "It was Hefter who first pointed out that man, irrespective of nationality, had rights and duties inherent in human nature and he was therefore not only a subject of international law but also a member of the international community." *Id.* at 104.

[48] *Id.* at 106. Individuals can be tried in international tribunals of competent jurisdiction. An example of how individuals can be hauled into court can be found with the prosecution of Nazi war criminals in the Nuremberg Trials at a special tribunal established for the purpose of such prosecutions. *International Military Tribunal (Nuremberg) Judgment and Sentences*, 41 AM. J. INT'L L. 172-75, 220-21 (1946), *reprinted in* HENKIN, *supra* note 46, at 360-63.

[49] TREATISE, *supra* note 46, at 107. Customary international law can be a norm of international law generally recognized as a crime by the international community, or it may be codified in the form of a bilateral treaty or multilateral convention. *Id.* at 106-07.

[50] *See supra* note 38.

[51] *Cf.*, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108 [hereinafter Convention for Data Protection]. (The convention does not directly apply to hacking, but may indirectly apply).

that renders the verdict as to his crime.[52] Extradition treaties can provide for broad extradition powers or, in the alternative, they can specify limited circumstances and offenses that are extraditable.[53]

Double criminality is a basic principle under international extradition law.[54] Double criminality means that "an act is not extraditable unless it constitutes a crime under the laws of both the state requesting extradition and the state from which extradition is requested."[55] Double criminality is vital in ensuring that a defendant's liberty is not restricted because of offenses not recognized as criminal in the state receiving the extradition request.[56]

Double criminality appears in one of two forms in extradition treaties. The traditional and most common form is where states limit extraditable offenses to those punishable under the laws of both states by a specified minimum term of imprisonment.[57] The second form, similar to the first form, limits the offense, but it also includes a particular list of non-extraditable offenses.[58]

The principle of double criminality poses a problem to punishing hacking on an international level. For hacking is not treated the same in all countries, and some countries have no laws addressing the computer violation.[59] Therefore, a loophole exists. If a hacker were to be a national and a resident of a country that does not have an anti-hacking law, it is possible that he could hack across international borders and be spared from extradition to the country whose computers were accessed.[60]

---

[52] TREATISE, *supra* note 46, at 138. "Extradition is the surrender of an individual accused or convicted of a crime by the state within whose territory he is found to the state under whose laws he is alleged to have committed or to have been convicted of the crime." HENKIN, *supra* note 46, at 885.

[53] *See generally* INTERNATIONAL CRIMINAL LAW: A GUIDE TO U.S. PRACTICE AND PROCEDURE 336-63 (Nanda & Bassiouni ed. 1987) [hereinafter Nanda & Bassiouni].

[54] *Id.* at 365. *See also* HENKIN, *supra* note 46, at 886.

[55] Nanda & Bassiouni, *supra* note 53, at 365 (citing SHEARER, EXTRADITION IN INTERNATIONAL LAW 137 (1971)).

[56] Nanda & Bassiouni, *supra* note 53, at 365.

[57] *Id.* at 366.

[58] *Id.*

[59] *See supra* note 38 and accompanying text.

[60] OECD, *supra* note 38, at 68.

D. *Mutual Assistance and the Hacker*

Treaties on mutual assistance address law enforcement and allow governments to go directly to other countries to seek assistance in gathering information.[61] Similar to extradition treaties, mutual assistance treaties may include limitations excluding the investigation of specified offenses.[62] Furthermore, some mutual assistance treaties apply the double criminality principle in that only offenses that are crimes in both countries can be mutually investigated.[63]

As applied to hacking, mutual assistance treaties can be paramount in international cooperation in punishing the offenders. As previously asserted, the hacker is usually in another country when he inflicts his damage. Therefore, the damaged country has no choice but to rely on the investigatory authorities of the hacker's home country.[64]

However, because mutual assistance treaties generally do not list hacking as an included offense and because hacking is not illegal in some countries, there are limits on the effectiveness of these treaties in punishing offenders.[65] Theoretically, a clever hacker can evade jurisdiction by knowing the laws of where he does his deed.

---

[61] Nanda & Bassiouni, *supra* note 53, at 233-34.

> [T]he treaties provide for a broad range of assistance in criminal matters, including: (1) executing requests relating to criminal matters, (2) taking testimony or statements of persons, (3) effecting the production, preservation and authentication of documents, records, or articles of evidence, (4) returning to the requesting party any objects, articles or any other property or assets belonging to it or obtained by the accused through criminal offenses, (5) serving judicial documents, writs, summonses, records of judicial verdicts and court judgments or decisions, (6) effecting the appearance of a witness or expert before a court of the requesting party, (7) locating persons, and (8) providing judicial records, evidence and information.

Id. at 236.

[62] *Id.* at 238-39. For example, judicial assistance may be refused when the execution of the request would prejudice the security or other essential interests of the state receiving the request. Also, some treaties deny assistance when the offense is purely military or political. *Id.* at 238.

[63] *Id.* at 236 n.10.

[64] An example of how a victimized country had no choice but to rely upon the investigatory authorities of another nation is found with the Australian incident, where United States officials were at the mercy of Australian officials to track down the hackers in Australia. *See supra* text accompanying note 5.

[65] *See supra* text accompanying note 60.

III. DOMESTIC LAW AND THE HACKER: THE "ENDS" AND "MEANS" APPROACHES

Due to the lack of international cooperation in apprehending and prosecuting hackers, domestic law is the sole source of bringing hackers to justice. Therefore, what follows is an examination into the treatment of hacking by domestic legal systems.

In general, countries approach computer hacking differently,[66] depending upon what actions are taken by the hacker when a system is accessed. The "ends" approach to computer hacking is when a country elects not to pass specific legislation prohibiting unauthorized access to a computer, based on the view that the computer is merely an instrument for committing an already illegal offense.[67] Basically, the "ends" of a hacker's conduct are illegal regardless of how the end result was achieved.[68]

In contrast, the "means" approach to hacking criminalizes "mere" access to a computer system without authorization.[69] Under the "means" approach, it is of no consequence whether an additional illegal act results from the unauthorized access.[70]

Although "ends" and "means" approaches hinge upon opposite foundations, the element of property is a common thread.

---

[66] Some countries are reluctant to modify existing laws to encompass computer crime either because the country has not experienced computer crime or it has determined the economic impact is too speculative and unknown. OECD, *supra* note 38, at 12. Other countries are more concerned with software piracy rather than unauthorized access. *Id.*

[67] The "ends" countries do not distinguish between information and computerized information. Their main concerns are computer security and compensation for damage done to private assets. *Id.*

[68] OECD members who have adopted the "ends" approach are Belgium, Iceland, and Japan. *Id.*

[69] *Id.* at 12, 61. Examples of specific computer statutes are found in the United States, Canada and the United Kingdom. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1988); Criminal Law Amendment Act, 1985, Act of June 20 1985, ch. C-19, § 301.2, 1985 Can. Stat. 272 (Unauthorized Use Of Computer); Computer Misuse Act, 1990, ch. 18 (LEXIS, International library, U.K. file). *See* Appendix for full text of Computer Misuse Act.

[70] OECD, *supra* note 38, at 12. Two attitudes exist behind the "means" approach. The first is to amend existing law provisions in order to encompass hacking. The second is to establish new incriminations to add the computer dimension. These two attitudes are not mutually exclusive. *Id.*

Prior to advancements in computer technology, existing laws offered adequate protection against the theft of information.[71] This protection stemmed from the fact that in order to steal information, the medium upon which it was written also had to be stolen.[72] The advent of computers, however, created a new problem encompassing the theft of information absent the theft of the medium.[73]

In countries that take the "ends" approach to computer hacking,[74] the property law element is glossed over in that computer data is deemed property.[75] In contrast, countries that attack the "means" of computer hacking reject the concept that computer data is property. "Means" countries statutorily attack the act of hacking in order to fill a void in inadequate property laws, such as those pertaining to theft and forgery, which the courts interpret not to protect information.[76]

Three common law countries illustrating the two approaches to hacking and the property dilemma are Canada, the United States and the United Kingdom.[77] While all three countries have specific computer statutes attacking the "means" of hacking, only Canada and the United States combat the "ends" as well. What follows is an analysis of the strengths and downfalls of each nation's approach.

IV. CANADA'S APPROACH TO HACKING

Canada takes both an "ends" and "means" approach to hacking, thus providing a strong statutory system against hacking on a domestic level.[78] Canadian law attacks the "ends" of

---

[71] OECD, *supra* note 38, at 29.

[72] *Id.*

[73] *Id.* Another problem existing between the information/medium dichotomy occurs with the admissibility of computer records as proof of their contents. MANN, *supra* note 43, at 179-80.

[74] *See supra* note 68 for a list of countries that follow the "ends" approach.

[75] OECD, *supra* note 38, at 12.

[76] For example, some cases in New York have held that computer-stored information is not property that can be stolen. Sokolik, *Computer Crime—The Need for Deterrent Legislation*, 2 COMPUTER/L.J. 353, 376 (1980).

[77] The following analysis will be limited to federal legislation because even though local legislation exists against hacking such local legislation does not apply internationally. *See generally* Soma, *supra* note 1; MANN, *supra* note 13.

[78] This is according to the Organisation for Economic Co-operation and Develop-

hacking through recently amended criminal statutes that regard computer data as property capable of being stolen.[79] Canadian law also attacks the "means" of hacking by criminalizing them under the Criminal Code section enacted in 1985 titled, Unauthorized Use of a Computer.[80]

A. *"Ends" Approaches*

1. *Theft Under the Criminal Code*

The Theft Section, section 283 of the Criminal Code,[81] provides, "everyone commits . . . theft who . . . converts to his use . . . anything whether animate or inanimate."[82] The words "animate or inanimate" clearly cover tangible and intangible property and thus enable charges to be brought against hackers[83] who print or save data[84] from illegally accessed systems.

Although no hacking cases have been considered under this section, one Canadian case applied the section to the copying of computer programs. In *Regina v. Tannas*,[85] the defendant was charged with theft when he converted for his use, computer programs belonging to his former employer, Dome Petroleum.[86]

---

ment. OECD, *supra* note 38, at 14.

[79] *See infra* notes 81-102 and accompanying text.

[80] *See generally* MANN, *supra* note 43, at 160-73.

[81] Criminal Code, R.S.C. 1970, c. C-34, § 283(1) provides:

> 283 (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate, with intent,
>
> (a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it,
>
> (b) to pledge it or deposit it as security,
>
> (c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform, or
>
> (d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

Id.

[82] *Id.*

[83] MANN, *supra* note 43, at 160-61.

[84] For example, the hacker could "download" the program to his own disk drive. "Download" is defined as "the process of transferring data from a large central computer system to a smaller, remote computer system." COMPUTER DICTIONARY, *supra* note 1, at 118.

[85] Alta. Q.B. (1984); *cited in*, MANN, *supra* note 43, at 163.

[86] MANN, *supra* note 43, at 163.

Although the jury found the defendant not guilty,[87] presiding Judge Bracco instructed the jury that computer software and the information contained on it were included in the phrase "anything that can be taken or converted."[88]

Tannas is significant for its underlying principle that the Canadian courts are willing to apply property laws to computer offenses.

2. *Mischief Under the Criminal Code*

Section 387(1) of the Canadian Criminal Code[89] makes it a crime to destroy or damage property, render property useless or inoperative or interfere with the lawful use or enjoyment of property. This section was applied to hackers in the case of *Regina v. Turner*.[90]

Turner involved hackers who accessed, from Toronto, the computer of a Milwaukee corporation.[91] The hackers inserted into the system a program that prevented the corporation's employees from gaining access to the stored information.[92]

The hackers argued that section 387(1) did not apply to their case because the statute was meant to cover real or tangible property.[93] The court disagreed, holding that the statute should be given its ordinary meaning.[94] Further, because the hackers made it impossible for the corporation to use or enjoy

---

[87] *Id.* at 164. Mr. Mann posits that this was because the prosecution did not prove its case. *Id.*

[88] *Id.*

[89] Criminal Code, R.S.C. 1970, c. C-34, § 387. The section provides:

387 (1) Every one commits mischief who willfully

(a) Destroys or damages property,

(b) renders property dangerous, useless, inoperative, or ineffective

(c) obstructs, interrupts, or interferes with the lawful use, enjoyment or operation of property, or

(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

Id.

[90] 27 B.L.R. 207 (Ont. H.C. 1984) *aff'd* Ont. C.A. (1985) *cited in* MANN, *supra* note 43, at 171.

[91] MANN, *supra* note 43, at 171.

[92] *Id.* at 171-72.

[93] *Id.* at 172.

[94] *Id.*

its property, the court found the hackers guilty of mischief.[95]

Turner illustrates Canada's approach to property law as including intangibles. After the *Turner* case, the Canadian legislature enacted an amendment to the statute, creating section 387(1.1), Mischief in Relation to Data, which in effect, codified the *Turner* holding.[96] This section prohibits the exact conduct in *Turner*, that of destroying or rendering data meaningless.[97] The amendment also is significant because it illustrates Canada's willingness to modify existing laws in order to accommodate computer offenses and to eliminate ambiguities that the courts may encounter.

3. *Personation Under the Criminal Code*

Section 361 of the Criminal Code,[98] Personation with intent, criminalizes impersonating someone for purposes of gaining an advantage, such as obtaining property, or to disadvantage another.[99] The section potentially could be applied to a hacker who uses an authorized user's password to access a system.[100]

Although no computer cases have been decided under this section, an impressive argument can be made that use of a password gives the hacker an advantage by entering a computer, while at the same time disadvantaging the authorized user by

---

[95] *Id.*

[96] Criminal Law Amendment Act, 1985, Act of June 20, 1985, ch. C-19 § 387(1.1), 1985 Can. Stat. 277. The section provides:

387 (1.1) 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
(d) obstructs, intercepts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Id.

[97] *Id.*

[98] Criminal Code, R.S.C. 1970, c. C-34, § 361. The section provides:

361 Every one who fraudulently personates any person, living or dead,
(a) with intent to gain advantage for himself or another person,
(b) with intent to obtain any property or an interest in any property, or
(c) with intent to cause disadvantage to the person whom he personates or another person
is guilty of an indictable offence and is liable to imprisonment for fourteen years.

Id.

[99] *Id.*

[100] MANN, *supra* note 43, at 169.

locking that person out of the system.[101]

Hypothetically, section 361 can be applied to the recent Australian hacking case. The Australians used a special program that stole and decoded passwords from a system file. Once decoded, the hackers used the passwords to access the files of authorized users.[102]

If the personation section were applied here, a conviction could be secured under the theory that the hackers intended to put the authorized users at a disadvantage when the hackers viewed the users' personal files. At the same time, the hackers intended to gain an advantage by using the password to enter the system. Although the statute is readily applied to the Australian case, it remains to be seen, whether Canada will apply it to hacking in the future.

B. *"Means" Approaches—Theft of Telecommunication Service Under the Criminal Code*

Prior to the enactment of stringent anti-hacking statutes, Section 287(1)(b) of the Canadian Criminal Code,[103] Theft of Telecommunication Services, was the sole governing authority when it came to attacking the "means." Section 287(1)(b) states it is theft if an unauthorized user "uses any telecommunication facility or obtains any telecommunication service."[104] The question of whether a computer is a "telecommunication facility" under section 287(1)(b) was addressed in *Regina v. McLaughlin*[105] and was answered in the negative.[106] In *McLaughlin*, an

---

[101] *Id.*

[102] *Password Plucker, supra* note 2, at A12.

[103] Criminal Code, R.S.C. 1970, c. C-34, § 287(1)(b). The section provides:

287 (1) Every one commits theft who fraudulently, maliciously, or without color of right,

(a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted or,

(b) uses any telecommunication facility or obtains any telecommunication service.

(2) In this section and in section 287.1,

"telecommunication" means any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire or cable.

Id.

[104] *Id.*

[105] 2 S.C.R. 331 (1980) *cited in* MANN, *supra* note 43, at 166.

[106] *Id.*

employee used a company computer for private purposes.[107]

In determining that the company computer was not a "telecommunication facility" under the statute, the Supreme Court of Canada held that the purpose of a computer was not to channel information outside, as is the function of a "telecommunication facility." Rather, the court maintained that computers are designed to retrieve and store information.[108] Hence, the mere fact that the outside user in *McLaughlin* used telephone lines to connect through a remote terminal[109] did not bring his conduct within the ambit of the section.[110]

Consequently, it is evident that the 287(1)(b) method of attacking the "means" to hacking was not without its loopholes. The above case illustrates that a hacker is outside the boundaries of prosecution under section 287(1)(b) unless the hacker actually devises a method to break into a telephone company network and charge telephone time to someone's account. However, quite often hackers do charge their intrusive activities to the accounts of others in order to avoid considerable telephone bills and to make tracing their telephone calls difficult.[111]

---

[107] MANN, *supra* note 43, at 166.

See, e.g., A. BEQUAI, COMPUTER CRIME 43 (1976). There two men had used their employer's computer to run their own music arranging business. The employees kept all of the records of the business on the employer's computer. *Id.*

In *McLaughlin*, even though the employee had accessed the computer by telephone like a hacker, access was authorized in that he used his own password. The difference was, once accessed, he used the computer for a purpose not authorized by his employer. MANN, *supra* note 43, at 166.

[108] MANN, *supra* note 43, at 166.

[109] *See supra* note 16 and accompanying text for definition of remote terminal.

[110] MANN, *supra* note 43, at 166.

[111] For example, in the most recent Australian arrests, the hackers charged all the long distance time to the accounts of the companies whose computers they had illegally accessed. *Global Peril*, *supra* note 2.

Another example are "Phone Phreaks" defined as "someone who likes to play with the phone system." Soma, *supra* note 1, at 573. Phreakers "specialize in using telephone equipment for their own use, free of charge. Through devices (such as blue boxes), they make toll-free calls around the world." *Id.*

Very often stolen credit card numbers or telephone account numbers are circulated on hacker bulletin boards so hackers make thousands of calls at no personal cost. FORESTER & MORRISON, COMPUTER ETHICS: CAUTIONARY TALES AND ETHICAL DILEMMAS IN COMPUTING 47 (1990).

C. *Filling Statutory Loopholes—Unauthorized Use of a Computer Under the Criminal Code*

To fill loopholes left by both "ends" and "means" statutes, the Canadian Legislature in 1985 enacted legislation aimed at the "means" of hacking. Section 301.2 of the Canadian Criminal Code,[112] Unauthorized Use of a Computer, makes it illegal to access a system without authorization. To date, no cases have been decided under the statute.

One commentator explains, however, the elements necessary to obtain a conviction under the statute.[113] To obtain a convic-

---

[112] Criminal Law Amendment Act, 1985, Act of June 20, 1985, ch. C-19, § 301.2, 1985 Can. Stat. 272. This section provides:

301.2 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 387 in relation to data or a computer system is guilty of an indictable offence and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section,

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other functions;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

Id.

[113] MANN, COMPUTER TECHNOLOGY AND THE LAW 173 (1987).

tion, it must be demonstrated that a hacker acted "fraudulently and without colour of right."[114] To prove such conduct, evidence must be introduced to show an intent to cause deprivation to another person.[115]

Further "it will also be noted that what is prohibited under paragraph 301.2(1)(a) is only the obtaining of a computer service (for example, data processing or the storage or retrieval of data) rather than the actual taking of computer data programs."[116] The section does not apply to "the retrieval of data belonging to [an]other person."[117] However, 301.2(1)(b) applies to "[t]he use of a device for the purpose of acquiring any data being communicated to, from or within a computer system . . . : This would be the case whether or not any information is in fact 'taken.' "[118] Therefore, this section purely attacks the "means" of computer hacking. Unlike section 287, convictions obtained under 301.2(1)(a) and (b) do not depend upon whether telephone time is illegally charged to the account of an unsuspecting victim.

The statutory sections specified above not only address the "means" of hacking, they also attack the "ends" by stating that it is illegal to destroy data as specified under Criminal Code section 387.[119] In addition, the statute includes a comprehensive list of definitions that may be helpful in avoiding ambiguities in court. Two such definitions include: "intercept"[120] and "Electromagnetic, acoustic, mechanical or other device."[121] Although it remains to be seen if section 301.2 will be tested against hacking, the all-encompassing nature of the statute's attack makes it a powerful domestic weapon in Canada's arsenal against computer crime.

In short, the Canadian Legislature aggressively combats the hacking problem by taking both "ends" and "means" approaches. However, one significant flaw is that Canada's statutory scheme fails to attack hacking on an international level. No

---

[114] *Id.*
[115] *Id.*
[116] *Id.* at 174
[117] *Id.* at 175.
[118] *Id.*
[119] *See supra* note 96; *See also supra* note 112.
[120] *See supra* note 112.
[121] *Id.*

sections provide for territoriality, extradition or double criminality as suggested by the Organisation of Economic Control and Development[122] and illustrated by the British Computer Misuse Act of 1990.[123] As the remaining sections of this Comment suggest, providing international protection is feasible as well as beneficial. Canada has the potential to reap benefits by adding statutory provisions dealing with international hacking issues.

V. The United States

The United States, like Canada, approaches hacking by attacking the "means." However, the United States launches a more reserved domestic attack against hacking, as compared to Canada, in that the United States fails to attack the "ends" of hacking through modified property statutes. In addition, weaknesses exist with the Federal Computer Fraud and Abuse Act,[124] the specific United States statute prohibiting hacking.

A. *Past Prosecution*

Prior to the enactment of the Federal Computer Fraud and Abuse Act, federal prosecutions were attempted under Federal Wire Fraud;[125] Federal Mail Fraud;[126] and, Federal Criminal Theft[127] statutes. All three are "ends" type statutes, and all were minimally successful in obtaining computer crime convictions. Each statute has its own pitfalls which impede the obtainment of hacking convictions. One particular problem is that the Federal statutes require that the hacking occur across state lines. Without this crossing of state boundaries, federal jurisdiction could not be obtained, and the statutes would be rendered inapplicable.[128]

---

[122] *See infra* text accompanying notes 265-287.

[123] The complete text of the British Computer Misuse Act of 1990 is reprinted at the Appendix to this Comment.

[124] 18 U.S.C. § 1030 (1988).

[125] 18 U.S.C. § 1343 (1988).

[126] 18 U.S.C. § 1341 (1988).

[127] 18 U.S.C. § 641 (1988).

[128] H.R. Rep. No. 894, 98th Cong., 2d Sess. 11, *reprinted in* 1984 U.S. Cong. & Admin. News 3689, 3691-92 [hereinafter Legislative History].

1. *Federal Wire Fraud Statute*

At one time, the Federal Wire Fraud Statute was useful for prosecuting hackers who used the wires to commit frauds.[129] The statute makes it a crime to perpetrate a fraud "for obtaining money or property by means of false or fraudulent pretenses . . . by means of wire, radio, or television communication in interstate or foreign commerce."[130]

The seminal case, *United States v. Seidlitz*[131] illustrates how the wire fraud statute applies to hacking. In this case, Seidlitz gained unauthorized access to the mainframe computer owned by Optimum Systems, Inc. (OSI), a Maryland corporation and Seidlitz's former employer. Seidlitz gained access by using an access code to the OSI system, which he learned when he worked at the firm.[132]

Upon accessing the system, Seidlitz copied[133] various parts of a program known as "WYLBUR."[134] Over a four-month period, Seidlitz accessed the system in OSI's Maryland office more than forty times from his Virginia office.[135] The fact that Seidlitz accessed the computer from across state lines enabled prosecutors to use the wire fraud statute on the basis that the access was gained through interstate commerce.[136]

One problem that the prosecutors encountered in using the wire fraud statute to prosecute Seidlitz was the statutory requirement mandating that the scheme be fraudulent for purposes of "obtaining money or property."[137] The court was faced

---

[129] A. BEQUAI, COMPUTER CRIME 38 (1978).

[130] 18 U.S.C. § 1343 (1988).

[131] 589 F.2d 152 (4th Cir. 1978) *cert. denied*, 441 U.S. 922 (1978).

[132] This unauthorized access is hacking and differs from the access cited in the Canadian case, Regina v. McLaughlin, 2 S.C.R. 331 (1980). Here, the employee's access was unauthorized by the employer, whereas Mr. McLaughlin's access was authorized. Mr. McLaughlin abused the authorization by using the computer system for personal reasons.

[133] He copied by downloading the program. *See supra* note 84 for a definition of downloading.

[134] BEQUAI, *supra* note 129, at 38. The WYLBUR program was used by the Corporation to obtain various government contracts. The program was one of the most sophisticated of the time. *Id.*

[135] *Id.*

[136] Legislative History, *supra* note 128, at 3692; *See also* BEQUAI, *supra* note 129, at 38.

[137] 18 U.S.C. § 1343 (1988). This section provides:

with the question of whether a computer program was property. In answering in the affirmative, the court noted that the program was used to obtain government contracts, making it a trade secret and therefore property.[138]

Despite the above-mentioned victory, the federal wire fraud statute is not without its downfalls. The statute is not effective against hackers, such as the Australian hackers, who do not copy programs in order to "obtain money or property."[139] If programs are simply copied by hackers for personal use, the question becomes whether the program can be considered "property" under the statute.

2. *Federal Mail Fraud Act*

A second statute used to prosecute computer offenses was the Federal Mail Fraud Act.[140] "This statute has two key elements that must be met: 1) use of the mails for the purpose of executing, or attempting to execute, 2) a fraud or scheme to obtain money or property under false pretenses."[141] Although this section applies to computer crimes, it would not apply to a ma-

---

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 5 years, or both.

[138] United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) *cert. denied* 441 U.S. 922 (1978).

[139] 18 U.S.C. § 1343 (1988).

[140] 18 U.S.C. § 1341 (1988). This section provides in pertinent part:

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, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

[141] BEQUAI, *supra* note 129, at 37.

jority of hackers because telephone lines, rather than the United States Postal Service, are used to commit hacking offenses.

A computer case in which this statute was applied was *United States v. Kelly*.[142] Here, the court held that the mailing of materials stored on the defendant's computer system, in order to perpetrate a fraud, was enough to constitute mail fraud.[143]

3. *Federal Criminal Theft Statute*

The Federal Criminal Theft Statute[144] was the most effective of the three statutes when it came to prosecuting computer crimes.[145] The statute makes it illegal to steal "any record . . . or thing of value."[146] The court interpreted a "thing of value" in *United States v. Girard*[147] to include intangible as well as tangible items.[148] The *Girard* case did not involve computers; rather it involved Girard's plan to secure information concerning the identity of government informants.[149]

Although the *Girard* court liberally applied The Criminal Theft Statute to favor the prosecution of computer crimes, the legislative history of the Computer Fraud and Abuse Act, enacted to fortify the United States' position against computer crime, indicates that such liberal construction was not the norm:

> As these computer technologies and the means for abusing them have rapidly emerged, they [courts] have been confronted by a criminal justice system which is largely uninformed concerning the technical aspects of computerization, and bound by tradi-

---

[142] 507 F. Supp. 495 (E.D.Pa. 1981).

[143] *Id.*

[144] 18 U.S.C. § 641 (1988). This statute provides in pertinent part:

> 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, or any property made or being made under contract for the United States or any department or agency thereof; or
>
> Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted
>
> . . . .

[145] Note, *Who Is Calling Your Computer Next? Hacker!* 8 CRIM. JUST. J. 89, 98 (1985) (authored by Diana Smith).

[146] 18 U.S.C. § 641 (1988).

[147] 601 F.2d 69 (2d. Cir. 1978) *cert. denied* 444 U.S. 871 (1979).

[148] *Id.*

[149] *Id.* at 70.

tional legal machinery which in many cases may be ineffective against unconventional criminal operations. Difficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft; a program, for example, may exist only in the form of magnetic impulses . . . . It is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes.[150]

B. *Present Prosecutions*

1. *Federal Computer Fraud and Abuse Act*

The three federal statutes mentioned above are "ends" based and only effective when hackers steal information or perpetrate frauds.[151] This legislative gap prompted Congress to pass a new statute, the Computer Fraud and Abuse Act.[152] The stat-

---

[150] Legislative History, *supra* note 128, at 3695.

[151] *Id.*

[152] 18 U.S.C. § 1030 (1988). This statute is an amended version of the original statute passed in 1984. The purpose of both statutes are identical. The 1986 statute was strengthened by adding definitions to terms that may be ambiguous in Court. The statute also added a category for destruction of computer data. *See generally* Tompkins and Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem* 6 COMPUTER/L.J. 459 (1986).

The 1986 statute provides:

1030. Fraud and related activity in connection with computers

(a) Whoever-

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains 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 section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et. seq.);

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is

ute's legislative history provides, in part:

---

used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

(5) intentionally accesses a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby-

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is-

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

There is no specific Federal legislation in the area of computer

---

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section-

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "Federal interest computer" means a computer-

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

(4) the term "financial institution" means-

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

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

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

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

(E) a member of the Federal home loan bank system and any home loan bank;

(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

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

crime. Any enforcement action in response to computer-related crime must rely on statutory restrictions that were designed for other offenses, such as mail fraud (18 U.S.C. § 1341) or wire fraud (18 U.S.C. § 1343) statutes. Even if an approach is devised that apparently covers the alleged acts in computer-related crimes, it still must be treated as an untested basis for prosecution in the Federal trial courts.[153]

The Computer Fraud and Abuse Act filled the legislative void of the "ends" statutes, by criminalizing the "means" of hacking, and made unauthorized access in and of itself illegal. The Act is limited in scope to computers of a "Federal interest."[154] Section 1030(e)(2) defines a Federal Interest computer as one used by the government, a financial institution of the government, or a computer that is one of two or more computers located in different states and used to commit an offense.[155] Therefore, jurisdiction is created only over the computers in the above categories.

The statute also prohibits unauthorized access to information that is adverse to National Security,[156] or to information

---

(H) the Securities Investor Protection Corporation;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter; and

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

[153] Legislative History, *supra* note 128, at 3691.

[154] Section 1030(e)(2) defines a Federal Interest computer as one;

(A) exclusively for the use of a financial institution of the United States Government, or in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same state. 18 U.S.C. §§ 1030(e)(2)(A) & (B) (1988).

[155] 18 U.S.C. § 1030(e)(1)(B) (1988).

[156] *Id.* at § 1030(a)(1).

contained in a financial record or consumer reporting agency.[157] Therefore, the statute pertains to hacking for fun, and it is of no legal consequence if a hacker's activities do not result in financial gain.[158] In addition, the statute also protects against destruction of or prevention of access to information in a Federal interest computer,[159] provided the damage to the victims is more than $1,000 during a one-year period.[160]

2. *The* Morris *Case*

The first successful prosecution under the Computer Fraud and Abuse Act was *United States v. Morris*.[161] The case involved a Cornell University graduate student studying computer science who unleashed a paralyzing computer worm program[162] on November 2, 1988, causing a virus to invade more than five thousand computers across the United States.[163] The case is paramount because it is only the second case tried under the Computer Fraud and Abuse Act[164] and the first successful conviction.[165]

---

[157] *Id.* at § 1030(a)(2).

[158] Although the statute does also have a provision forbidding stealing by computer. *Id.* at § 1030(a)(4).

[159] *Id.* at § 1030(a)(5).

[160] *Id.*

[161] No. 90-1336 (D.C.N.Y. 1990) *aff'd* 928 F.2d 504, (2d Cir. 1991). *See also* Kane, *Sorcerer's Apprentice Meets Less Benign Fate*, Nat'l L.J., Feb. 5, 1990, at 8, col. 1.

[162] Basically, a worm program is a computer instruction or small hidden program inserted on a standard computer program or into a computers operating system. Note, *supra* note 145, at 627. These instructions may reproduce many times during a single program execution, infect every program on a computer disk and be passed on secretly to other computers through modems, floppy disks, or network connections. *Id. See also* LEGISLATIVE BUDGET AND FINANCE COMMITTEE, REPORT TO THE PA GENERAL ASSEMBLY OF 1988, 8 (1988).

The reason why Mr. Morris' worm program was so devastating was because it was written in binary code, which is the language of electronic impulses that computers use to communicate. This code is very difficult for programmers to break down. Kane, *supra* note 161.

[163] Kane, *supra* note 161. The virus attacked the network of Internet, the same network the most recent Australian hackers penetrated. *Id.*; *See also Global Peril*, *supra* note 2, at A16.

[164] 18 U.S.C. § 1030 (1988). See Kane, *supra* note 161 for the other case, United States v. Doe, 88-CR-672 (1988).

[165] Kane, *supra* note 161, at 8. Mr. Morris was convicted on January 22, 1990. *Id.* He was sentenced to three years probation and 400 hours of community service on May 4, 1990. United States District Judge Howard Munson also ordered him to pay a $10,000

As with the Australian hackers, Morris said he unleashed the program to magnify the security problems existing in the infected computer systems, and his intention was not to disable the systems.[166]

The *Morris* case illustrates the typical hacking offense and the resultant damage. The disabled computer systems that were shut down throughout the United States[167] meant that a significant number of businesses, universities, and even NASA could not operate. The result was millions of dollars in losses.[168]

Like the Australian hackers, Morris stole[169] the passwords of authorized users to the systems, thus blocking legitimate access.[170] In addition, the damage caused by Morris's worm program required corrections at the expense of hundreds of overtime hours.[171] Because of the extensive damage, Morris was charged and convicted under section 1030(a)(5)(A) of the Act[172]

---

fine plus court and probation costs. This was a lenient sentence under the Act considering the maximum sentence is five years and $250,000 in fines. Schaefer, *Computer Hacker Gets Probation, Fine*, United Press International, May 5, 1990 (NEXIS, U.P.I. library).

[166] Kane, *supra* note 161, at 8. Hackers are very often breaking into computer systems to show a company that security problems exist. Usually, the hacker will acknowledge this fact by posting a message once inside the system proving that he got inside. Note, *supra* note 145, at 94.

Some have said a hacker is a blessing in disguise because they argue he performs a valuable public function in exposing security flaws in computer systems. *Id.* However, it is generally recognized that hackers should give notice to companies before attempting to perform this "public service." Mr Morris did not attempt to give notice until after he found out his program had gone awry. Kane, *supra* note 181.

[167] Kane, *supra* note 161.

[168] *Id.*

[169] *See supra* note 35 and accompanying text for discussion of stealing passwords.

[170] Kane, *supra* note 161, at 8; *See also* Schulkins, *The Electronic Burglar*, 1 COMPUTER L. & PRAC. 140 (1985).

[171] Kane, *supra* note 161, at 8. A worm is a form of a virus. A virus requires many hours of work for computer operators to rid the system of it. This type of damage can also occur when hackers browse. For example, in one case, hackers gained access to the records of an intensive care ward in a Los Angeles hospital and altered the patients records by doubling all patients doses of medication. Although no damage was done, it took dozens of medical and computer personnel to review the 6,000 patient files in the hospital to be sure no tampering had occurred. Mann, *supra* note 113, at 158-59. Prevention of this type of alteration of medical records is codified at 18 U.S.C. § 1030(a)(5)(B) (1988). See *supra* note 152 for the text of this prohibition.

[172] 18 U.S.C. § 1030(a)(5)(A) provides:

(a) whoever—

(5) intentionally accesses a Federal interest computer without authoriza-

for "gaining unauthorized access to computers, preventing their use and causing losses in excess of $1,000."[173]

A potential weakness in the statute that was highlighted by the *Morris* case was the element of "intent." The section of the statute under which Morris was charged renders it unlawful to "intentionally access a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information . . . ."[174]

In this case, the sophistication of Morris's program indicated that he clearly did not intend to cause the damage.[175] His actual intent was to expose security flaws in the systems entered.[176] If the program had not gone awry, the damage would not have occurred.[177]

The Court interpreted the definition of intent to include the "means" of Morris' actions. District Judge Howard G. Munson instructed the jury that "[t]he government need not prove that it was the defendant's intention to prevent access to computers or to cause damage to those computers."[178] Notably, Morris' conviction was possible because the Computer Fraud and Abuse Act is a "means" statute and consequently the only matter of legal concern was that Morris utilized his computer to cause the damage.

Morris' conviction has been upheld on appeal. Therefore, Judge Munson's instructions pertaining to "intent" were lawful.[179] *Morris* demonstrates that the United States is now serious about preventing domestic computer crime by attacking its "means." The fact that Morris' crime was generated via a computer is the hinging factor dictating a United States emphasis on "means" as opposed to "ends."

---

tion, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby-

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period . . . .

[173] Kane, *supra* note 161, at 8.

[174] 18 U.S.C. § 1030(a)(5) (1988).

[175] Kane, *supra* note 161, at 8.

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] United States v. Morris, 928 F.2d 504, (2d Cir. 1991).

3. *Criticisms of the Computer Fraud and Abuse Act*

Morris' conviction under the Computer Fraud and Abuse Act does not guarantee that all incidents of hacking will be prosecuted. Scholars have criticized the statute as not comprehensive enough.[180] First, it has been suggested that the monetary amounts be repealed because a hacker may not cause $1,000 of damage if mere browsing[181] occurs. Second, if a hacker accessed a non-Federal interest computer, then jurisdiction does not attach.[182] Consequently, a loophole is left open for hackers who browse non-Federal interest computers within state boundaries. Under this scenario, a hacker's activities would go unprosecuted unless prohibited by state law.[183]

Third, the act fails to define key terms, including: "access," "authorization," "use," and "affects."[184] This failure potentially creates ambiguities for District Courts to wrestle with.[185]

Fourth, the definition that does exist creates a de minimis exception under the Act.[186] The instrumentality addressed by the act is a "computer."[187] The Act specifically excludes typewriters, calculators, and "other similar devices"[188] that are usually not excluded from definitions of computers.[189] The definition is weak because in the future, "other similar devices" may be used to commit hacking offenses and remain beyond prosecu-

---

[180] *See* Tompkins & Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Persuasive Problem*, 6 COMPUTER/ L.J. 459 (1986).

[181] *Id.* at 472. Browsing has been called "computer trespass", or browsing at files or data.

> For example, if a person breaks into the Pentagon computers and just views the top secret information, it is not a crime. In order to violate the Act in this case, the person would have to obtain the information with the intent or reason to believe that the information will be used to harm the United States.

Note, *Computer Crime and the Computer Fraud and Abuse Act of 1986* 10 COMPUTER/ L.J. 71, 79-80 (1990) (authored by Christopher D. Chen) [hereinafter Chen].

[182] *See supra* text accompanying notes 154-55. This is interesting because non-Federal interest computers are corporate computers which are arguably subject to the most abuse, yet are virtually ignored under the Act. Chen, *supra* note 181, at 79-80.

[183] Soma, Smith & Sprague, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571, 603 (1985) [hereinafter Soma].

[184] Tompkins & Mar, *supra* note 180, at 476.

[185] *Id.*

[186] *Id.* at 463.

[187] 18 U.S.C. § 1030(e) (1988).

[188] *Id.* at § 1030(e)(1).

[189] Tompkins and Mar, *supra* note 180, at 463.

tion. Also, difficulty in interpreting the term may come about.

However, the federal statute improves upon the approach to hacking prior to its enactment. Overall, the United States may not be far behind Canada in the prosecution of hacking offenses on the domestic level because many states have anti-hacking laws.[190] However, hackers who know the laws can avoid prosecution by taking advantage of jurisdictions that do not criminalize their acts.

In short, the United States federal and state systems have narrowed the hacking that can occur without violation of a statute.[191] Questions remain as to whether a hacker who does not cause damage can be convicted and whether the statute will have a deterrent effect. The recent Australian incident is not a positive sign that these statutes actually deter.

In addition, the United States statute, like the Canadian provisions, does nothing to prevent hacking on an international level because provisions for territoriality, extradition or double criminality are not included.

VI. The United Kingdom

The United Kingdom's legal system prosecutes hacking differently as compared with the United States and Canada in that its domestic system is not as strong in attacking the "ends" of hacking. England has not modified its property laws to attack hacking. However, the Computer Misuse Act[192] was recently enacted to punish the "means" of hacking. This statute approaches hacking on an international scale. In addition to this assured global protection, England also has a unique statute, The Data Protection Act,[193] which theoretically can be applied to international hacking. To date, however, The Data Protection Act has

---

[190] Soma, *supra* note 183, at 621.

[191] In addition, Congress introduced legislation to criminalize computer viruses, entitled "The Computer Virus Eradication Act of 1989." This legislation will be an amendment to the Computer Fraud and Abuse Act and would aim to further punish activity such as that undertaken by Robert Morris that spreads viruses through computers. *See generally* Note, *The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues*, 3 Software L.J. 717-53 (1990).

[192] Computer Misuse Act, 1990, ch. 18 (Lexis, International library, U.K. file). *See* Appendix.

[193] *See infra* text accompanying notes 225-234.

not been used for that purpose.

A. *Attempted Prosecutions*

The case of *Regina v. Gold and Schifreen*[194] illustrates the inadequacy of the English property laws in combatting hacking. The case was decided by the High Court and was unsuccessful in prosecuting hackers under the Forgery and Counterfeiting Act of 1981.[195] The case is one of global magnitude in illustrating the problem of "ends" oriented prosecution of the hacker who causes no damage.

The case arose when Gold and Schifreen, two juvenile hackers, broke into the Prestel system[196] in England by figuring out passwords and user codes of authorized users.[197] The prosecution contemplated conviction of the defendants upon deception grounds,[198] but, under English law, deception must occur against a human being.[199] Here, the only deception that occurred was against a computer. The defendants tricked the computer into believing that they were the Duke of Edinburgh and thus were able to leave a message in the Duke's electronic mailbox.[200]

The prosecution attempted conviction under the Forgery and Counterfeiting Act of 1981,[201] instead of upon deception grounds. The Forgery and Counterfeiting Act prohibits the creation or use of a forged instrument with the intention of causing

---

[194] [1987] 3 W.L.R. 803. *See also* Lloyd, *Computer Abuse and The Law* 104 THE L.Q. REV. 202 (1988); Nicholls, *Hacking and the Criminal Law* 3 COMPUTER L. & PRAC. 64 (1986); Kwiatkowski, *Hacking and the Criminal Law Revisited*, 4 COMPUTER L. & PRAC. 15 (1987); Kwiatkowski, *British Telecom Hackers Vindicated*, 4 COMPUTER L. & PRAC. 172 (1988) [hereinafter *British Telecom*].

[195] Forgery and Counterfeiting Act, 1981, ch. 45.

[196] Lloyd, *supra* note 194, at 202. This system is owned by British Telecom and offers a variety of data bases to customers. The customer is supplied with a password and user code to gain access. This system is much like CompuServe in the United States. *Id.*

[197] The defendants tried unsuccessfully to convince British Telecom that the Prestel System was not secure. Therefore, in order to prove their point, they broke into the Prestel electronic mailbox of the Duke of Edinburgh. *British Telecom*, *supra* note 194, at 173. The purpose of illustrating an unsecured system was also the motivating factor behind the Australian hacker's and Mr. Morris' actions of hacking.

[198] Lloyd, *supra* note 194, at 203.

[199] *Id.* (citing Davies v. Flackett, [1973] R.T.R. 8).

[200] Lloyd, *supra* note 194, at 203.

[201] Forgery and Counterfeiting Act, 1981, ch. 45.

another "to do or not to do some act to his own or any other person's prejudice."[202]

An "instrument," under the Act, is defined, *inter alia*, as "any disc, tape, soundtrack or other device on or in which information is recorded or stored by mechanical, electronic or other means."[203] An instrument is false "if it purports to have been made in the form . . . by a person who did not in fact make it in that form,"[204] or "if it purports to have been made in the form . . . on the authority of a person who did not in fact authorise its making in that form . . . ."[205]

To secure a conviction, the prosecution had to identify the false instrument that the defendants allegedly created.[206] Consequently, an attempt was made to identify the password as the instrument.[207] The court held, however, that the electronic impulses a computer produces are not devices "on or in which information is . . . stored," and thus passwords are not instruments.[208] As a result of this determination, the court overturned the trial court's conviction of the defendants.[209]

The case illustrates the problems faced by countries without modified "ends" laws deeming information to be property. The case further illustrates the need for "means" statutes. Because in this instance no damage occurred, the leaving of the unauthorized message in the Duke's electronic mailbox could not be prosecuted under the United Kingdom's "ends" statute.

B. *The Computer Misuse Act of 1990*

Realizing the need for domestic legislation to attack hacking and to prevent England from becoming an "international hackers' haven,"[210] Michael Colvin (C, Romsey and Waterside) introduced in Parliament legislation aimed at preventing the com-

---

[202] *Id.* at pt. I, § 3.
[203] *Id.* at pt. I, § 8(1)(d).
[204] *Id.* at pt. I, § 9(1)(a).
[205] *Id.* at pt. I, § 9(1)(b).
[206] *British Telecom*, *supra* note 194, at 173.
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Bill to Curb Hacking Sent to Lords*, *The Daily Telegraph*, May 5, 1990, at 11 (NEXIS, CURRNT library).

puter crime. On June 29, 1990, Parliament passed Colvin's legislation, The Computer Misuse Act of 1990.[211] The stated purpose of the Act is "to make provision for securing computer material against unauthorised access or modification . . . ."[212]

The Act creates three offenses: causing a computer to perform any function with intent to gain access to any program or data held in any computer;[213] committing the above offense with intent to commit or facilitate the commission of a further offense;[214] and causing an unauthorized modification of the contents of any computer.[215]

On a domestic level, the Computer Misuse Act criminalizes the "means" of hacking by prohibiting mere access to a computer system. A hacker causes a computer to perform a function with intent to gain access when he enters passwords during the process of accessing a system.[216]

The Computer Misuse Act expands the "ends" approach by criminalizing the use of computers for illegal conduct, including acts beyond unauthorized access.[217] Attacking the "ends" via this statute however, is not as effective as modifying property statutes, as Canada has done. For example, if a hacker robs a bank by using his computer to transfer funds, he will only be subject to prosecution under The Computer Misuse Act.

As such, the hacker is subject to a five-year prison sentence under the Act[218] and will avoid potentially stiff penalties under "ends" bank robbery statutes. In short, no matter what "end" damage results, a hacker is subject only to a five-year sentence under the Computer Misuse Act.

Finally, the Computer Misuse Act penalizes hackers who

---

[211] The Computer Misuse Act, 1990, ch. 18 (Lexis, International library, U.K. file). See Appendix for the full text. The Act came into force on August 29, 1990.

[212] *Id.* at Long Title.

[213] *Id.* at § 1.

[214] *Id.* at § 2.

[215] *Id.* at § 3. Modification of the contents of a computer if data held in the computer is altered or erased or any program or data is added to its contents. *Id.* at §§ 17(7)(a) & (b). This modification is unauthorized if the person's actions causing the modification is not entitled to determine whether the modification should be made, or if that person does not have consent to modify. *Id.* at §§ 17(8)(a) & (b).

[216] Wasik, *Tackling Technocrime: The Law Commission Report on Computer Misuse*, 6 COMPUTER L. & PRAC. 23, 24 (1989) [hereinafter *Tackling Technocrime*].

[217] Computer Misuse Act, 1990, ch. 18, § 2.

[218] *Id.* at § 2(5)(b).

unleash viruses into a computer system, by making it illegal to tamper with the contents of a computer.[219] Therefore, the *Morris* incident,[220] for example, is illegal under the Act.

Due to the fact that the Computer Misuse Act has been enacted recently, no cases yet have tested its applicability under English law. However, once the Act is tested there is every indication that it will prove to be highly effective in attacking hacking on an international scale.

First, the Act contains provisions dealing with jurisdiction and the territorial problems associated with hacking.[221] Second, the Act states that British citizenship is immaterial in its application to hacking offenses.[222] Finally, the Act includes provisions for extradition[223] and double criminality.[224] Therefore, the Computer Misuse Act contains strong, albeit untested, provisions concerning the international aspects of both the "ends" and "means" of hacking.

C. *The Data Protection Act*

In addition to the Computer Misuse Act, the United Kingdom's Data Protection Act of 1984[225] may be applicable to hacking offenses, although no situation has presented itself to this date.[226] The main purpose of the Data Protection Act is to protect individuals' right to know if personal information pertaining to them is being stored in an "agency's" computer.[227] Individuals

---

[219] *Id.* at § 3.

[220] *See supra* notes 161-179 and accompanying text.

[221] Computer Misuse Act, 1990, ch. 18, § 4.

[222] *Id.* at § 9.

[223] *Id.* at § 15.

[224] *Id.* at § 8(1).

[225] Data Protection Act, 1984, ch. 35. *See also* Howe, *Data Protection in the United Kingdom*, 3 COMPUTER L. & PRAC. 204 (1987); Chalton, *Data Protection: New Civil Liberty, or Heffalump Trap?*, 1 COMPUTER L. & PRAC. 31 (1984); Burkert, *Institutions of Data Protection-An Attempt at a Functional Explanation of European National Data Protection Laws*, 3 COMPUTER/L.J. 167 (1981); Raymont, *Information Technologies: A Challenge to the Individual and to the Enterprise*, 1 COMPUTER L. & PRAC. 22 (1984).

[226] OECD, *supra* note 38, at 21. The Organisation for Economic Co-operation and Development states the Act "could be applicable because its principle that personal data must be adequately secured may lead to increased emphasis on computer security all around." *Id.*

[227] Data Protection Act, 1984, ch. 35, pt. III, § 21. *See also* Howe, *supra* note 225, at 204.

who know of such information being stored further have the right to ensure that the information is accurate.[228]

The Data Protection Act theoretically can be applied to hacking because it provides for civil and criminal penalties for the wrongful disclosure of information about an individual.[229] The Act calls for adequate security measures, without specifying what is deemed adequate, in order to protect from wrongful disclosure of personal information stored on computer systems.[230] Therefore, it is theoretically possible under the Data Protection Act to penalize[231] a holder of personal information, rather than a hacker, if a hacker should acquire unauthorized access to personal information collected about an individual.

The Data Protection Act however, has numerous exemptions to the requirement that computer systems storing personal information must be secure. Thus, all computer systems are not under the jurisdiction of the Act.[232]

The Act has not yet been applied to hacking incidents. One possible explanation for this is that the Act punishes the victims of the crime rather than the perpetrator. Furthermore, fewer hacking incidents may be reported than actually occur because the one who reports the hacking is subject to penalties under the Act.

Despite the above, the Organisation for Economic Co-operation and Development in its study of computer crime asserted that the Act could lead to increased emphasis upon computer

---

The Act requires any agency that holds information on individuals to register with a Registrar of Data. Data Protection Act, 1984, ch. 35, pt. II, § 4(1).

[228] Howe, *supra* note 225, at 204. This part of the Act is aimed at ensuring that credit information, for one, is accurate. *Id.* at 205-06.

[229] Data Protection Act, 1984, ch. 35, pt. II, § 15(1). This section provides that "[p]ersonal data in respect of which services are provided . . . shall not be disclosed . . . without the prior authority of the person for whom those services are provided." *Id. See also Id.* at sched. I, which sets up the principles underlying the Data Protection Act.

[230] *Id.* at sched. I, pt. 1, § 8 which provides: "8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data."

[231] Penalties under the Act include both civil remedies and criminal penalties. One provision of the Act allows an individual to be compensated as a result of unauthorized information that is disclosed. *Id.* at pt. III, § 23(1). Another provision holds the director, manager, secretary or similar officer of a corporation criminally liable under the Act. *Id.* at pt. II, § 20(1).

[232] *See id.* at pts. III & IV.

security.[233] The Organisation's theory leads to another explanation as to why few cases exist; that is, computer systems are secured as required by the Data Protection Act. This eliminates the need and increases the difficulty for hackers to expose security flaws.

In summary, England must modify its current "ends" property statutes, as evidenced by the *Regina v Gold and Schifreen* case, in order to have a domestic system comparable to Canada's in attacking computer crime.[234] However, there is hope in that the Computer Misuse Act of 1990 is a strong "means" statute. When coupled with the Data Protection Act, the combination may be adequate to combat hacking domestically without the need for modifying "ends" statutes. Furthermore, the Computer Misuse Act is exemplary in approaching hacking on an international level.

VII. SOLUTIONS

A. *Security*

The Australian arrests illustrate security problems that exist with computer systems.[235] The security problems, in addition to the English Data Protection Act, raise the question of whether an adequate solution to hacking is the enactment of laws compelling owners of computer systems to secure the systems and holding them liable for break-ins into non-secured systems. Going hand-in-hand with such statutes compelling security would have to be statutes requiring mandatory reporting of computer crimes to appropriate authorities.[236]

The disadvantage of such a system is that the victims of the crime would not only be violated by hackers, but would also bear penalties should they choose not to report their victimization. This raises equitable arguments as to such a system's validity in that it deprives computer owners of freedom of choice.

First, a corporation may be willing to bear the risk of a hacker breaking into its system because the amount of economic

---

[233] OECD, *supra* note 38, at 21.

[234] *See supra* text accompanying notes 194-209.

[235] *See Global Peril*, *supra* note 2.

[236] *See Scottish Law Commission: Report on Computer Crime*, 3 COMPUTER L. & PRAC. 27, 28 (1987).

damage done will be minimal in comparison to the cost of either: establishing a security system; or the damage to its corporate reputation if publicity should result from the hacking.[237] Second, no security system can be absolutely safe. There is always a chance that someone will hack the system.[238] Therefore, security alone, without legislative action, will not be sufficient to conquer the problem.

In contrast, there are advantages to compelling computer users to secure their systems. Such is a reasonable measure because it will force awareness of security lapses, and thus further the ultimate desire of deterrence of hacking.[239] Deterrence of hacking would occur if users are compelled to secure computers, because the difficulty of hacking would increase. Thus, the hacker's self-imposed mission of exposing security flaws would be eliminated.[240]

Different security measures have been suggested by the United States Government.[241] One recommendation it that computer owners identify an individual who is responsible for information security.[242] Other methods are: to secure,[243] manage[244]

---

[237] These corporations gamble that the risk of loss is less than the cost of the benefits derived from a secure system. An example of this would be a personal computer owner who has a modem hooked up to his computer, but feels security is not really necessary. *See* Schulkins, *Who Needs Security?*, 1 COMPUTER L. & PRAC. 65, 66 (1984); J. CARROLL, COMPUTER SECURITY 10-12 (1977).

Also, as seen from the legislative history of the United States Computer Fraud and Abuse Act, the corporation may be concerned that the publicity will lead to more hackers trying to enter the system because they know it is an easy target. Legislative History, *supra* note 128, at 3697.

[238] Schulkins, *supra* note 237, at 65.

[239] Price-Waterhouse conducted a survey in 1985 which indicated that system security was lacking in U.S. corporations. The Survey examined 131 Companies and indicated that twenty-five percent (25%) provided adequate security systems while the remaining seventy-five percent (75%) failed to employ security at all. Note, *Who is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 110 (1985) (authored by Diana Smith).

[240] *See generally* A. BEQUAI, HOW TO PREVENT COMPUTER CRIME (1983); U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, COMPUTER SECURITY TECHNIQUES (1982); PREVENTION COMMITTEE, PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY, COMPUTERS: CRIMES, CLUES, AND CONTROLS (1986) [hereinafter PREVENTION COMMITTEE]; D. PARKER, CRIME BY COMPUTER (1976); J. CARROLL, COMPUTER SECURITY (1977); U.S. CONGRESS, OFFICE OF TECHNOLOGY AND ASSESSMENT, DEFENDING SECRETS, SHARING DATA: NEW LOCKS AND KEYS FOR ELECTRONIC INFORMATION (1987) [hereinafter TECHNOLOGY ASSESSMENT].

[241] PREVENTION COMMITTEE, *supra* note 240, at 9-19.

[242] *Id.* at 37.

[243] *Id.* at 15. This includes employees not sharing passwords, choosing passwords

and create multi-level passwords;[245] to keep remote systems off when not in use;[246] to restrict the files and information that can be accessed by certain people;[247] to keep logs for the system;[248] to limit the number of incorrect passwords acceptable to a system before disconnection;[249] and to investigate frequent system crashes.[250]

Other systems for security are "call-back" systems;[251] encryption or scrambling program systems;[252] "read only" systems;[253] and "token-based" systems.[254] This is by no means a

---

hard to guess, letting the computer generate passwords, and mixing letters and numbers in creation of passwords. *Id.*

[244] *Id.* at 16. This includes changing passwords periodically and on an irregular schedule, assigning password access to trusted officials only, invalidating passwords when officials leave the company, and protecting the files that have password access. *Id.*

[245] This is basically requiring more than one password to be entered before access is obtained. *See supra* note 35 and accompanying text for the definition of a password.

[246] PREVENTION COMMITTEE, *supra* note 240, at 17.

[247] *Id.* at 16.

[248] *Id.* at 13. Logs are "[a] record of operations of a computer system listing each job or run, the time it required, operator actions, and other pertinent data." COMPUTER DICTIONARY, *supra* note 1, at 214. These logs were the files the Australian hackers erased to conceal their identities. *Global Peril*, *supra* note 2.

This is also done by Audit Trails which "maintain an ongoing record of who is using the system and what major actions are performed. The system's operators can then review this 'audit trail' to determine unusual patterns of activity (e.g., someone consistently using the system after office hours) or to reconstruct the events leading to a major error or system failure." TECHNOLOGY ASSESSMENT, *supra* note 240, at 86.

[249] PREVENTION COMMITTEE, *supra* note 240, at 17. Basically this is limiting the number of attempts to enter a password and access the system to, for example, two or three attempts, or the phone connection will automatically terminate. *Id.*

[250] *Id.* at 14. A system crash is "(1) The cessation of the operation of a computer. (2) A system shutdown caused by a hardware malfunction or a software mistake." COMPUTER DICTIONARY, *supra* note 1, at 79. This is a symptom of a computer virus.

[251] This is a system where the computer terminates the connection once access is achieved by a remote user. After termination, the computer will dial the pre-programmed phone number of the authorized user. Schulkins, *The Electronic Burglar*, 1 COMPUTER L. & PRAC. 140, 141 (1985).

[252] These programs prevent hackers from breaking into a valid connection between an authorized user and remote computer. The information is scrambled and appears as "garbage" on the hackers' computer terminal. *Id.* at 140.

[253] This system prevents data alteration by remote access. The system enables a hacker to browse the data, but not alter it. The only individual authorized to change the data is the one with the passwords to the writing files. Note, *supra* note 239, at 110.

[254] This system has a device that is hooked up to the remote user's system which generates a digital "token." The "token" is similar to a password but randomly generated by the "token" device and is unknown to the remote user. This system allows the host computer to determine if the computer attempting access is authorized. TECHNOL-

complete list of security systems, and many new systems are being developed for better security in the future.[255]

In summary, a law compelling security would not be inequitable because the burden of complying with such a statute would be minimal due to existing technology for computer security. One possible solution is to deem personal information holders liable for security lapses as does the English Data Protection Act. However, a necessary addition to such a requirement is the enactment of a second statute requiring mandatory reporting of hacking. Without such a combination of legislation, the United Kingdom's approach will accomplish concealment, rather than conquering of hacking. If all computer users employed security systems, hacking to expose security flaws would be unnecessary and thus international hacking would be less of a problem.[256] In addition, hacking without detection would be more difficult.[257]

B. *International*

As illustrated by the recent Australian arrests, security is not instituted worldwide. Therefore, hacking occurs on a global scale. An examination of hacking prevention measures that have been and can be employed globally is therefore in order.

1. *Convention for the Protection of Individuals*

Although there has been no conventions directly addressing hacking, one applicable convention is the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[258]

OGY ASSESSMENT, *supra* note 240, at 74-77.

[255] One such system being developed is the Biometric and Behavioral Identification System. This system identifies a user by a biological aspect, such as the retina pattern of the user's eye. *Id.* at 77-83.

[256] The Australian case illustrates this type of hacking. *Global Peril*, *supra* note 2.

[257] Again as the Australian incident illustrates, the hackers were not detected for two years because they had written a program that erased the security files that were used to keep track of who had logged onto the system. Many of the security files, however, were easy to enter. If more advanced security and tracking systems were used, such as the types listed above, the hackers would have had a much more difficult time in both entering the security files and escaping detection.

[258] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data at Strasbourg, Jan. 28, 1981, Europ. T.S. No. 108 [hereinafter Convention].

As with the United Kingdom's Data Protection Act,[259] the Convention's main concern is the protection of "personal data."[260] Article 1 of the Convention states its object and purpose in a nutshell: "The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."[261]

Article 7 is concerned with data security.[262] Basically, the Article requires holders of personal data to use appropriate security measures to protect data against unauthorized destruction or access.[263]

As with the English Data Protection Act, this Convention, Article 7 in particular, places the burden of preventative measures on the holder of information. Therefore, the risk assessment option available to a computer owner is eliminated.

The problem with this Convention in application to hacking is that not all computer systems hold "personal data," and thus security for all systems is not required. The lack of universal security for all computer systems will not alleviate the problem but will simply reduce the available number of systems that can be penetrated.

On a final note, the best of security systems is inadequate without one additional crucial ingredient—world cooperation. As illustrated by the Australian hacking incident, the world must cooperate to criminalize hacking and send a message that hack-

---

As of March 1988, countries who signed the convention were:
Austria, Belgium, Cyprus, Denmark, France, F.R. Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, and The United Kingdom. *Data Protection Update* 4 COMPUTER L. & PRAC. 136 (1988).

[259] *See supra* text accompanying notes 225-34.

[260] "Personal data" is defined in Article two of the convention as "any information relating to an identified or identifiable individual ('data subject') . . . ." Convention, *supra* note 258, at art. 2(a).

[261] *Id.* at art. 1.

[262] *Id.* at art. 7. Article 7 provides: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination." *Id.*

[263] *Id.*

ers will be prosecuted for their misconduct.[264]

2. *OECD Suggestions*

The Organisation for Economic Co-operation and Development (OECD)[265] has conducted an analysis of legal policy concerning computer crime.[266] This analysis includes suggestions on how to eliminate international hacking.

The study's introduction explains a prime reason behind its initiation is "[t]o try to reach a common understanding both of computer-related crime itself and of how the law can deal with it."[267] The remainder of this section will summarize the solutions to hacking as suggested by OECD.

a. *Legislative — Domestic*

New legislation must be passed worldwide[268] because even if hacking does not occur within a single nation, hacking is an international dilemma of which every nation is a potential victim.[269] The legislation should punish both the "means" as well as the "ends" of hacking.

As far as legislation that punishes the "means," OECD suggests, first, a specific statutory provision criminalizing mere ac-

---

[264] One of the Australian hackers falsely believed he was not chargeable with a felony for his hacking. International cooperation like that of a convention would aid in educating hackers that the world is serious about preventing their crime. *Global Peril*, *supra* note 2.

[265] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 10 COMPUTER RELATED CRIME: ANALYSIS OF LEGAL POLICY (1986) [hereinafter OECD].

[266] *Id.*

[267] *Id.* at 7.

[268] OECD, *supra* note 265, at 38-39.

[269] This again is illustrated by the Australian incident. The computer systems penetrated were in the United States. Because Australian legislation gives Australia jurisdiction over hacking from Australia into other countries, the hackers could properly be arrested under the scope of that legislation. *Global Peril*, *supra* note 2. If Australia did not have specific legislation aimed at the "means" of hacking, the United States would not have been able to reach the hackers outside of attempting extradition procedures for violation of "ends" statutes.

The most recent Dutch situation illustrates this very dilemma. The Netherlands does not have a specific "means" statute, so the United States is forced to rely on extradition procedures based on violation of "ends" statutes by the hackers. *See Dutch Rogues*, *supra* note 8.

cess.[270] The rationale behind such provisions is that they are identical to criminal statutes that prohibit conduct such as copying a key[271] or entering real property without causing damage.[272]

Second, the mere access statute must be coupled with a "wiretapping" provision criminalizing use of national or international telephone lines to commit a computer offense. Such a provision is necessary because the telephone lines are needed not only to obtain unauthorized access, but also to obtain authorized access.[273]

OECD explains that a "premium" may be granted to well-intentioned hackers who gain unauthorized access to computer systems in order to illustrate the lack of security.[274] This "premium" may take the form of special consideration at the time of prosecution and would apply only to hackers who give immediate notice to the victim or to the appropriate state authorities of their illicit access and of the loopholes they discovered.[275] Such a provision might benefit computer owners in that hackers will not feel restricted in their self-imposed mission to find and point out security flaws. The downfall of the "premium" is that it fails to address the invasion of privacy and property that results when an unauthorized user obtains access to a system. Furthermore, hackers might be tricked into a false sense of security by believing their activities are covered under the "premium" only to learn that their well-intentioned intrusion caused damage, therefore falling within the full realm of prosecutorial penalties under "means" statutes.

Third, a specific statutory provision criminalizing alteration or destruction of data must be included.[276] Two examples of such a provision are found with the Canadian Mischief in Rela-

---

[270] OECD, *supra* note 265, at 60-63.

[271] *See, e.g., Id.* at 61 (citing C. PEN., § 399 (France)).

[272] OECD, *supra* note 265, at 61.

[273] *Id.*

[274] *Id.* at 63. It is worth noting that Canada, the United States and the United Kingdom do not have statutory provisions providing leniency for well-intentioned hackers in their "means" statutes. *See* Criminal Law Amendment Act, 1985, Act of June 20 1985, ch. C-19, § 301.2, 1985 Can. Stat. 272 (Canadian Unauthorized Use of Computer Statute); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1988); Computer Misuse Act, 1990, ch. 18.

[275] OECD, *supra* note 265, at 63.

[276] *Id.* at 39.

tion to Data Statute[277] and the English Computer Misuse Act of 1990.[278]

In addition to "means"-oriented solutions, modification or creation of statutory provisions attacking the "ends" of hacking also must be passed with the inclusion of computer data in the definition of "property."[279] The most common "ends" statutes in need of modification are those dealing with theft,[280] larceny, embezzlement and credit card fraud.[281]

A further type of "ends" statutes in need of modification are those dealing with fraud. Fraud provisions must be modified or created to include computer fraud.[282] OECD has suggested that fraud statutes criminalize "the manipulation of data with the intent to deprive another in order to gain illegal profit . . . ."[283]

Additional "ends" statutes in need of modification are those dealing with treason.[284] Treason statutes should specifically protect "[s]ensitive military, technological and diplomatic information . . . ."[285] An anti-hacking treason provision would penalize hackers who access government computers containing information regarding national security.[286]

Finally, both "means" and "ends" statutes must express definitions in terms of function, rather than technology, in order to remain current with the rapidly-changing technological advancements of computer hardware and software.[287]

b. *Collective — International*

Two general principles required by the international community are: an international unification of efforts to keep transborder data flows[288] moving freely; and the protection of per-

---

[277] *See supra* note 96 and accompanying text.

[278] *See* Appendix.

[279] OECD, *supra* note 265, at 40-43.

[280] This should also include theft of trade secrets via computer. *Id.* at 47.

[281] *Id.* at 39-40.

[282] *Id.* at 39.

[283] *Id.*

[284] *Id.* at 46.

[285] *Id.*

[286] *Id.*

[287] *Id.* at 40.

[288] *See, e.g.*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDE-

sonal data collected about individuals.[289] Further, OECD's stated policy dictates that international economic transactions be protected.[290]

"The development of data bank interconnections via international telecommunications networks brings an international dimension to computer-related crime."[291] A person at a terminal in country A could manipulate a program or access a computer in country B, and through such conduct affect the interests in Country C.[292]

The territorial principle dictates jurisdiction in the circumstances specified above.[293] That is, the applicable law is that of the country in which the offense or one of its elements is alleged to have occurred.[294] It is apparent that the hacking problem affects the territorial principle because an element of an offense may occur in all three countries, thus creating trilateral jurisdiction. In addition, the principle of "Non bis in idem"[295] is applicable. OECD suggests that these problems be addressed by coordinating international efforts.

One solution to the global hacking problem is incorporating clear jurisdictional provisions into computer statutes.[296] Besides the English Computer Misuse Act,[297] an example of such a jurisdictional provision can be found in a currently existing Scottish "means" statute.[298]

The jurisdictional section of this Scottish statute grants jurisdiction to Scotland to try an offender "[w]here the offences . . . are committed partly in Scotland and partly in another country . . . irrespective of whether at the material time he was

---

LINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1981).

[289] *See, e.g.*, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108.

[290] OECD, *supra* note 265, at 2.

[291] *Id.* at 66

[292] *Id.*

[293] *Id.*

[294] *Id.*

[295] "Not twice for the same; that is, a man shall not be twice tried for the same crime." BLACKS LAW DICTIONARY 948 (5th ed. 1979).

[296] OECD, *supra* note 265, at 66-67.

[297] *See* Appendix.

[298] *See Scottish Law Commission: Report on Computer Crime*, 4 COMPUTER L. & PRAC. 27, 28 (1987).

himself in Scotland or in that other country."[299]

Second, international efforts may be coordinated by clearly stating provisions for choice of law and extradition procedures.[300] Such provisions will give hackers the impression that a unified front among nations is against them.

Third, international efforts may be coordinated through expansion of extradition treaties to specifically include computer offenses as extraditable.[301] Extradition treaties should be written in such a manner to obligate extradition if a warrant is issued and the offense is a felony.[302]

Finally, international efforts must be coordinated through mutual assistance between countries.[303] Mutual assistance concerns the investigation of alleged hacking offenses and includes such elements as search and seizure, service of documents, or the taking of testimony or statements of citizens of other nations.[304]

In short, "[t]hese issues deserve further consideration by Member countries[305] and appropriate international bodies."[306] "[I]nternational co-operation in repressing and controlling [hacking] activity . . . "[307] is necessary. The most forceful type of international cooperation would be a specific convention prohibiting hacking. However, such a convention is not necessary if each nation alters its existing treaties.

VIII. Conclusion

The global hacking phenomenon is illustrated by the Australian arrests of April 2, 1990.[308] The case is a prime example of the level of international cooperation necessary to combat hacking effectively. In that incident, computers within the United

---

[299] *Id.*

[300] OECD, *supra* note 265, at 67.

[301] *Id.*

[302] *Id.*

[303] *Id.* at 68.

[304] *Id.* An example of this mutual assistance is again illustrated by the recent Australian incident. The authorities of Australia and the United States cooperated in apprehending the hackers who damaged computer systems in the United States from Australia. *Global Peril*, *supra* note 2.

[305] See OECD, *supra* note 265, at 2 for a list of OECD Member countries.

[306] *Id.* at 70.

[307] *Id.*

[308] *See supra* text accompanying notes 1-14.

States were damaged by hackers operating out of Australia. In prosecuting the hackers, the United States cooperated with Australian authorities. Once the hackers were traced, the Australian authorities charged the hackers with an offense under Australian law.

The incident illustrates the problems with current hacking statutes. If Australia did not have a specific hacking statute, the hackers would have been beyond prosecution unless the United States sought extradition. The problem with relying upon extradition is twofold: 1) the principle of double criminality and 2) tracing the hackers without Australian assistance. In absence of a hacking statute, Australian police would lack investigatory jurisdiction and United States authorities could not rely upon Australian assistance to extradite the hackers. Further, the United States could not even request extradition of the Australian citizens even though hacking is illegal in the United States under the Computer Fraud and Abuse Act.

The exact dilemma stated above has presented itself in the most recent Dutch hacking incident. In that incident, Dutch hackers penetrated United States computers hooked to Internet. The hackers caused no damage in their escapade, and the Netherlands has no law prohibiting the "means" of hacking. Therefore the United States can not reach the hackers in the Netherlands.[309]

The suggested solutions by OECD will solve the above-mentioned problems. If every nation passes a specific computer statute against hacking in accordance with the OECD guidelines calling for extradition and mutual assistance clauses, the problems would not exist and investigations similar to that in the Australian/United States incident would be common.

However, because international cooperation is still but a dream, domestic law is the sole source of prosecuting the computer crime of hacking. Of the three systems examined, Canada's is the strongest domestically because it has modified "ends" statutes to attack the damages resulting from hacking. Canada also attacks the "means" of hacking and punishes hackers who do not necessarily cause any damage when they penetrate computer systems.

---

[309] *See Dutch Rogues*, *supra* note 8.

The United States system is adequate for attacking hacking on a domestic level. The United States does not attack the "ends" of hacking as effectively as the Canadian system because its "ends" property statutes do not specifically include hacking damage as criminal. The United States attacks hacking primarily through its "means" statute, the Computer Fraud and Abuse Act. However, that statute is not as strong as it could be because it is federal and thus does not criminalize hacking within state boundaries. The statute also does not define key terms: hence there is room for potential ambiguities to be litigated. Finally the statute does not account for future technological changes. Nevertheless, the statute to date has been successful in convicting at least one computer hacker.

Finally, the United Kingdom's domestic system in attacking the "ends" of hacking is weak because its property statutes do not include computer offenses. The United Kingdom's "means" statute, The Computer Misuse Act, is powerful, however, in protecting the United Kingdom from both domestic and international hackers. The United Kingdom's "means" statute, internationally, has provisions providing for extradition, double criminality and mutual assistance. Such a statute is necessary in attacking hacking on a global level. Other countries could benefit from following the United Kingdom's statutory example.

Domestically, the United Kingdom potentially protects personal data from hacking invasions through the Data Protection Act. This Act compels holders of personal information to adequately secure their computer systems and could eliminate a hacker's self-proclaimed mission of exposing security flaws. The problem with such an Act is that it could result in victim's concealing hacking incidents, rather than the conquering of hacking offenses.

On an international level, the only convention that applies—the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data—relies on the same theory as the United Kingdom's Data Protection Act. The theory is that the responsibility lies with the holder of information to protect the information from hackers. Within a single country that theory may be sound, but again, the international hacking problem is not addressed. Only a three-prong attack with combined "ends," "means," and data protection laws man-

dating security will effectively eliminate hacking on a global scale.

On a final note, hacking is a global crime unlike one that was ever experienced. The linking of the world through common networks has created the problem. The only effective resolutions are: 1) to sever the international connection; or 2) to keep the world linked and cooperate to prevent the abuses that result. The world has the choice.

ROBERT J. SCIGLIMPAGLIA, JR.

APPENDIX

COMPUTER MISUSE ACT, 1990, CH. 18.

The following is the full text of the English Computer Misuse Act which was passed on June 29, 1990 and went into force on August 29, 1990.

SECTION: Long Title

Text:

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

SECTION: 1 Unauthorised access to computer material

Text:

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on a standard scale or to both.

SECTION: 2 Unauthorised access with intent to commit or facilitate commission of further offences

Text:

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

SECTION: 3 Unauthorised modification of computer material

Text:

(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite

knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

SECTION: 4 Territorial scope of offences under this Act

Text:

(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

(4) Subject to section 8 below, where—

(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references—

(a) in the application of this Act to England and Wales, to England and Wales;

(b) in the application of this Act to Scotland, to Scotland; and

(c) in the application of this Act to Northern Ireland, to Northern Ireland.

SECTION: 5 Significant links with domestic jurisdiction

Text:

(1) The following provisions of this section apply for the interpretation of section 4 above.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at the time.

(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification; or

(b) that the unauthorised modification took place in the home country concerned.

SECTION: 6 Territorial scope of inchoate offences related to offences under this Act

Text:

(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's

guilt—

(a) the question where any person became a party to the conspiracy; and

(b) the question whether any act, omission or other event occurred in the home country concerned.

(2) On a charge of attempting to commit an offense under section 3 above the following questions are immaterial to the accused's guilt—

(a) the question where the attempt was made; and

(b) the question whether it had an effect in the home country concerned.

(3) On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt.

(4) This section does not extend to Scotland.

SECTION: 7 Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.

Text:

(1)-(3) . . .

(4) Subject to section 8 below, if any act done by a person in England and Wales would amount to the offence of incitement to commit an offence under this Act but for the fact that what he had in view would not be an offence triable in England and Wales-(a) what he had in view shall be treated as an offence under this Act for the purposes of any charge of incitement brought in respect of that act; and

(b) any such charge shall accordingly be triable in England and Wales.

ANNOTATIONS:

Sub-ss (1), (2): amend the Criminal Law Act 1977, s.1.

Sub-s (3): amends the Criminal Attempts Act 1981, s.1.

SECTION: 8 Relevance of external law

Text:

(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Law Act 1977 only if the pursuit of

the agreed course of conduct would at some state involve—

(a) an act or omission by one or more of the parties; or

(b) the happening of some other event;

constituting an offence under the law in force where the act, omission or other event was intended to take place.

(3) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Attempts Act 1981 or by virtue of section 7(4) above only if what he had in view would involve the commission of an offence under the law in force where the whole or part of it was intended to take place.

(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(5) Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice—

(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to show that it is satisfied.

(6) In subsection (5) above "the relevant conduct" means—

(a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;

(b) where the condition in subsection (2) above is in question, the agreed course of conduct; and

(c) where the condition in subsection (3) above is in question, what the accused had in view.

(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.

(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.

(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.

(10) In the High Court of Justiciary and in the sheriff court

the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.
SECTION: 9 British citizenship immaterial
Text:

(1) In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

(2) This section applies to the following offences—

(a) any offence under this Act;

(b) conspiracy to commit an offence under this Act;

(c) any attempt to commit an offence under section 3 above; and

(d) incitement to commit an offence under this Act.

SECTION: 10 Saving for certain law enforcement powers
Text:

Section 1(1) above has effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.

SECTION: 11 Proceedings for offences under section 1
Text:

(1) A magistrates' court shall have jurisdiction to try an offence under section 1 above if—

(a) the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time.

(2) Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge.

(3) No such proceedings shall be brought by virtue of this section more than three years after the commission of the

offence.

(4) For the purposes of this section, a certificate signed by or on behalf of the prosecutor and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(5) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(6) In this section "commission area" has the same meaning as in the Justices of the Peace Act 1979.

(7) This section does not extend to Scotland.

SECTION: 12 Conviction of an offence under section 1 and in proceedings for an offence under section 2 or 3

Text:

(1) If on the trial on indictment of a person charged with—(a) an offence under section 2 above; or

(b) an offence under section 3 above or any attempt to commit such an offence;

the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.

(2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 1 above as a magistrates' court would have on convicting him of the offence.

(3) This section is without prejudice to section 6(3) of the Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment).

(4) This section does not extend to Scotland.

SECTION: 13 Proceedings in Scotland

Text:

(1) A sheriff shall have jurisdiction in respect of an offence under section 1 or 2 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which

the accused secured or intended to secure unauthorised access by doing that act was in the sheriffdom at that time.

(2) A sheriff shall have jurisdiction in respect of an offence under section 3 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the unauthorised modification; or

(b) the unauthorised modification took place in the sheriffdom.

(3) Subject to subsection (4) below, summary proceedings for an offence under section 1, 2 or 3 above may be commenced within a period six months from the date on which evidence sufficient in the opinion of the procurator fiscal to warrant proceedings came to his knowledge.

(4) No such proceedings shall be commenced by virtue of this section more than three years after the commission of the offence.

(5) For the purposes of this section, a certificate signed by or on behalf of the procurator fiscal and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(6) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(7) Subsection (3) of section 331 of the Criminal Procedure (Scotland) Act 1975 (date of commencement of proceedings) shall apply for the purposes of this section as it applies for the purposes of that section.

(8) In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence commenced before the expiry of any time limit under this section applicable to such proceedings.

(9) Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.

(10) A person found guilty of an offence under section 1 above by virtue of subsection (8) above shall be liable, in respect

of that offence, only to the penalties set out in section 1.

(11) This section extends to Scotland only.

SECTION: 14 Search warrants for offences under section 1

Text:

(1) Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing—

(a) that an offence under section 1 above has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises;

he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.

(2) The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in section 9(2) of the Police and Criminal Evidence Act 1984 (privileged, excluded and special procedure material).

(3) A warrant under this section—

(a) may authorise persons to accompany any constable executing the warrant; and

(b) remains in force for twenty-eight days from the date of its issue.

(4) In exercising a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.

(5) In this section "premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.

(6) This section does not extend to Scotland.

SECTION: 15 Extradition where Schedule 1 to the Extradition Act 1989 applies

Text:

The offences to which an Order in Council under section 2 of the Extradition Act 1870 can apply shall include—

(a) offences under section 2 or 3 above;

(b) any conspiracy to commit such an offence; and

(c) any attempt to commit an offence under section 3 above.

SECTION: 16 Application to Northern Ireland

Text:

(1) The following provisions of this section have effect for

applying this Act in relation to Northern Ireland with the modifications there mentioned.

(2) In section 2(2)(b)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to section 33 of the Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the Magistrates' Courts (Northern Ireland) Order 1981.

(3) The reference in section 3(6) to the Criminal Damage Act 1971 shall be read as a reference to the Criminal Damage (Northern Ireland) Order 1977.

(4) Subsections (5) to (7) below apply in substitution for subsections (1) to (3) of section 7; and any reference in subsection (4) of that section to England and Wales shall be read as a reference to Northern Ireland.

(5) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

(1B) Paragraph (1A) applies to an agreement if—

(a) a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;

(b) a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or

(c) a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;

and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions.".[sic]

(6) The following paragraph shall be inserted after paragraph (4) of that Article—

"(5) In the application of this Part to an agreement to which paragraph (1A) applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence tria-

ble in Northern Ireland.

(6) In this Article "computer misuse offence" means an offence under the Computer Misuse Act 1990.".[sic]

(7) The following paragraphs shall be inserted after Article 3(1) of that Order—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.

(1B) Paragraph (1A) above applies to an act if—

(a) it is done in Northern Ireland; and

(b) it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.".[sic]

(8) In section 8—

(a) the reference in subsection (2) to section 1(1A) of the Criminal Law Act 1977 shall be read as a reference to Article 9(1A) of that Order; and

(b) the reference in subsection (3) to section 1(1A) of the Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.

(9) The references in section 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.

(10) In section 11, for subsection (1) there shall be substituted—

"(1) A magistrates' court for a county division in Northern Ireland may hear and determine a complaint charging an offence under section 1 above or conduct a preliminary investigation or preliminary inquiry into an offence under that section if—

(a) the accused was in that division at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in that division at that time.";

and subsection (6) shall be omitted.

(11) The reference in section 12(3) to section 6(3) of the Criminal Law Act 1967 shall be read as a reference to section 6(2) of the Criminal Law Act (Northern Ireland) 1967.

(12) In section 14—

(a) the reference in subsection (1) to a circuit judge shall be read as a reference to a county court judge; and

(b) the reference in subsection (2) to section 9(2) of the Police and Criminal Evidence Act 1984 shall be read as a reference to Article 11(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989.

ANNOTATIONS:

Sub-ss (5)-(7): amend SI 1983 No 1120, arts 3, 9.

SECTION: 17 Interpretation

Text:

(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform-(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if—

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

SECTION: 18 Citation, commencement etc

Text:

(1) This Act may be cited as the Computer Misuse Act 1990

(2) This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.

(3) An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.

Computer Misuse Act, 1990, ch. 18 (Lexis, International library, U.K. file).