TO WHAT EXTENT SHOULD COMPUTER RELATED CRIMES BE THE SUBJECT OF SPECIFIC LEGISLATIVE ATTENTION?

Douglas H. Hancock

INTRODUCTION

The general proposition in most common law jurisdictions is that criminal laws are to be construed narrowly. If there is any doubt as to whether or not the activity complained of is a criminal act, then the judicial result must favor the liberty of the accused. This basic tenet of criminal law has been further enshrined in many common law jurisdictions by the codification of the criminal law. If it is not in the criminal code, then it is not

a criminal matter.[1]

This essentially laudable, almost motherhood principle, has not always coped well in the fluid technological context of modern Western commercial society. Activities not even imagined twenty years ago must be analyzed based on laws formulated in past centuries. While the common law has continued to adapt to civil disputes, criminal laws and their interpretation have often been ill-equipped to deal with unforeseen human activities.

The House of Lords has affirmed the legal view that the judiciary should be reluctant to create new criminal laws, although it does, strictly speaking, have such authority.[2] That task is, in their view, reserved principally to the legislature.[3] This approach has been followed in most Western jurisdictions.[4] Thus in scenarios which do not fit neatly within the ambit of existing criminal laws, there is the likelihood that the activity will not be viewed as being subject to criminal censure. This conclusion will be reached although there may well be a consensus in society that the conduct is reprehensible.

---

[1] ROLAND N. BOYCE & ROLLIN M. PERKINS, CASES AND MATERIALS ON CRIMINAL LAW AND PROCEDURE 988 (7th ed. 1989) (explaining ex post facto laws, "[A] person shall not be punished on a criminal charge for an act that was no offense at the time it was performed.").

[2] See Shaw v. Dir. Of Pub. Prosecutions, [1962] A.C. 220, 268 (H.L. 1961) (appeal taken from Eng.) (explaining the court's authority to create new criminal laws, "[T]here is in th[e] court a residual power, where no statute has yet intervened to supercede the common law, to superintend those offences which are prejudicial to the public welfare.").

[3] See id. ("Such occasions will be rare, for Parliament has not been slow to legislate when attention has been sufficiently aroused.").

[4] Note, Common Law Crimes in the United States, 47 COLUM. L. REV. 1332, 1334 (1947)(explaining the judiciary's reluctance to innovate and apply criminal laws that have not been codified).

WHAT IS COMPUTER RELATED CRIME?

The use of a computer is a narrow, and potentially misleading, aspect of what is meant by computer related crime. For example, using a computer as a blunt instrument when committing an assault is, obviously, not a computer crime. Conversely, there are a variety of scenarios that do not involve a computer per se, but nonetheless fall within the ambit of computer related crime.

Most definitions of the term computer acknowledge its two main functions; namely, the ability to store data and the ability to process data.[5] The absence of either function normally leads to the conclusion that the device is not a computer as such. For example, a calculator is not a computer.[6] However, a variety of hand-held devices (although performing relatively crude tasks in comparison to their relatively sophisticated counterparts) probably do constitute computers.

The United States Department of Justice has identified six areas where crimes are facilitated by the computer and by the Internet:

---

[5] Law Commission, Working Paper No. 110, Computer Misuse, 1988, at 7. See also id. at 126-128 (listing the definition of computer from the United States, Canada, Isreal, and Tasmania). See also Webopedia: Online Computer Dictionary for Internet Terms and Technical Support, (defining "personal computer" as, inter-alia, "a keyboard for entering data, a monitor for displaying information, and a storage device for saving data") available at http://www.webopedia.com/TERM/c/computer.html (last visited Oct. 14, 2001).

[6] 18 U.S.C. §1030(e)(1)(1994) (excluding "an automated tywriter or typesetter, a portable hand held calculator, or similar device" from the definition of "computer").

(1) Use of the actual computer to facilitate a crime;

(2) Internet gambling;

(3) Cyberstalking and harassing speech;

(4) Unlawful conduct on the Internet;

(5) Child pornography; and

(6) Sale of prescription drugs over the Internet.[7]

To the categories listed by the Department of Justice, one could also add the following:

(1) Unauthorized access to computer networks;

(2) Creation and dissemination of viruses;

(3) Denial of service attacks; and

(4) Unauthorized sale of copyright protected material.

The definition of a computer crime must, out of necessity in an ever changing technological context, be a fluid concept. Not all crimes committed with a computer are computer crimes. The Report of the President's Working Group on Unlawful Conduct on the Internet gave this example to illustrate this point, "If someone steals a telephone access code and makes a long distance call, the code they have stolen is checked by a computer before the call is processed. Even so, such a case is more appropriately treated as 'toll fraud', not computer crime."[8]

[7] See United States Dep't. of Justice, Computer Crime and Intellectual Property Section (CCIPS), available at http://www.cybercrime.gov/crimes.html (last visited Oct. 14, 2001).

[8] The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (A Report of the President's Working Group on Unlawful Conduct on the Internet) at 10 (Mar. 2000), available at http://www.cybercrime.gov/unlawful.htm (last visited Oct. 14, 2001) [hereinafter Frontier].

Ultimately the crux of the issue is that the computer play some role in facilitating the crime. Obviously, the computer can play various roles. It can be the target of the crime itself, as it would be in the case of an attack by a virus. It may be simply a storage device for unlawful activities. Conversely, it may act as the conduit to implement the crime - probably as a communication tool for voice and data.[9]

Given such a broad, almost all encompassing definition, it follows that existing criminal laws will cope adequately in certain jurisdictions in some scenarios. The instances when existing criminal laws fail to adequately protect the public, (or are at least perceived by the public in that manner) are of academic and practical interest.

THE PROBLEMS - PERCEIVED AND REAL

The penetration of the computer into homes and businesses coupled with the growth of the Internet have concurrently abetted the criminal world by facilitating criminal activities.[10] United States Attorney General, Janet Reno, stated that "While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behavior."[11] The Internet has the potential to make every user a published author and every person with a computer now has a medium to disseminate information. The downside to

[9] See id. at 9-10.
[10] See id. at 3.
[11] Id. at 4.

this scenario has been demonstrated in many instances when individuals have used message boards to manipulate the price of securities traded on stock exchanges.

One of the more clever schemes involved posting a message about Pargain, a telecommunications company, on a Yahoo! message board together with a link to what appeared to be a website of the Bloomberg News Service.[12] The website contained a detailed story about the pending takeover of Pargain by an Israeli Company.[13] The website proved to be a hoax, but only after the price of the stock went through huge gyrations; a thirty percent increase in value followed by a sharp decline, resulting in tremendous financial loss.[14]

The Internet's veritable empowerment of the individual has at the same time made commercial enterprises vulnerable. A teenager from Montreal Canada, self-styled the "Mafiaboy", singlehandedly brought CNN and other high profile web sites to a standstill.[15] The goals of "Mafiaboy" and his counterparts were probably not new, but having the mechanisms literally at their finger tips to actually carry out their misdeeds certainly was.

In a similar vein, the Internet is also facilitating traditional crimes. Mail and telephone fraud may now be perpetrated more efficiently and cost effectively via e-mail. The fraud itself may not be new, but the means and ease of delivery are. Pyramid

[12] See id. at 5-6.
[13] See id.
[14] See id. at 6.
[15] See Ariana Eunjung Chaand & David Streitfeld, Microsoft Web Sites Attacked; Company Asks FBI for Assistance, WASH. POST, Jan. 26, 2001, at E1, available at 2001 WL 2539619, at *3.

schemes can now reach millions of potential victims in a multitude of jurisdictions, rather than hundreds in one or two countries.[16] The multi-jurisdictional aspect of many of these crimes adds to the difficulties faced by law enforcement agencies. Traditional crimes that are merely facilitated by computers are generally excluded from definitions of computer crimes.

The extent of computer misuse is generally cited as the one of the most compelling arguments for specific legislation.[17] The New Zealand Law Commission has noted that the extent of the problem is likely understated by businesses for fear of publicity.[18] One source has estimated that less than five per cent of all computer offenses are reported.[19] Commerce now depends in large part upon the ability to freely exchange information electronically. If the integrity of that exchange is imperiled, then quite literally the underpinning of Western commercial society is placed in jeopardy.

---

[16] See generally, Kathy Fieweger "Make Thousands of Dollars from Home!" Screams the Classified Ad. "A Great Income Opportunity!" Says the Email From the Unknown Sender.; "Want to Earn Hundreds of Dollars A Week -- At Home in Your Leisure Time?" Asks the Flyer Stuck on a Telephone Pole, CHI. TRIB., Dec. 31, 2000, at 1, available at 2000 WL 29791088, at *2 (describing pyramid schemes by drawing an analogy to envelope-stuffing opportunities). These work at home offers require a processing fee in order to receive work, but what one is told to do is to advertise the same offer in newspapers or send it to acquaintances. The money comes from charging the same fee. [hereinafter Fieweger]. See also Jon Swartz, Scam Artists Thriving on the Internet, SAN FRANCISCO CHRONICLE, Dec. 20, 1997, at E1, available at 1997 WL 6713477, at *1 (reflecting on the growing concern that the Internet provides criminals with millions of potential victims worldwide).

[17] Law Commission of New Zealand, Report 54, Computer Misuse, 1999, at 2 [hereinafter Report 54].

[18] See id. at 10.

[19] International Review of Criminal Policy - Nos. 43 and 44, United Nations Manual On The Prevention and Control of Computer-Related Crime, p.8 available at http://www.ifs.univic.ac.at/~pr2gq/rev4344.html.

Hacking is often cited as a prime example of what is meant by computer misuse.[20] Hacking involves gaining access to a computer network without proper authorization.[21] The manner in which access is gained and what the protagonist does once he or she has gained access will have a bearing on whether or not the conduct is subject to censure.[22] Nonetheless, all such activities have produced a veritable sub-culture amongst hackers. A recent search using the Yahoo! search engine revealed 118 web site matches.[23]

A website [24] devoted to the ethics of "hackers", quotes Steven Levy author of, Hackers: Heroes of the Computer Revolution. Mr. Levy states that his tenets are as follows:

(1) Access to computers should be unlimited and total.

(2) All information should be free.

(3) Mistrust authority - promote decentralization.

(4) Hackers should be judged by their hacking not bogus criteria

such as degrees, age, race, or position.

(5) You create art and beauty on a computer.

[20] See Frontier, supra note 8 at 10.
[21] See id.
[22] See id. at 10-11 (presenting varieties of networks that are being illegally accessed, and the sensitive information involved). The report describes the theft of sensitive information from law enforcement and military networks. Id. The report also discusses the theft of information from enforcement of non-governmental systems, such as businesses, for credit card numbers; intellectual property theft involving trade secrets; and telephone networks for long distance access. Id.
[23] Conducted on October 14, 2001.
[24] The Hackers Ethic, available at Http://hoshi.cic.sfu.ca/~guay/Paradigm/Hacker.html (last visited Oct. 14, 2001).

(6) Computers can change your life for the better.[25]

The home page of the web site concludes by noting that the "Internet as a whole reflects this ethic."[26]

The exploits of hackers are numerous and often high profile. A synopsis of the so-called achievements of hackers is clearly outside the parameters of this undertaking. However, by way of example, hackers have gained access to virtually all of the most ostensibly well-guarded sites on the Internet. As of 1995, the United States Defense Department's computer had been penetrated via the Internet more than 160,000 times.[27]

Similarly, web sites of businesses that hold confidential information as an integral aspect of their business have been vulnerable.[28] The Canadian loyalty program, Air Miles, saw its confidential customer data disseminated to the public on its web site thanks to the efforts of a hacker.[29] This information included sensitive personal information on all Air Miles members, such as telephone numbers and addresses.[30]

Hackers can gain access in a number of different ways. How access is obtained may be relevant in deciding whether or not a criminal offence has been committed. The technique may be as

[25] Id.
[26] Id.
[27] See Report 54, supra note 17, at 11.
[28] See id. (indicating that 190 of 200 businesses surveyed in 1995 admitted being the victims of computer fraud).
[29] See Michael Geist, H is for Hackers: an A to Z guide to cyberlaw in 1999 (Dec. 23, 1999) available at http://newsglobetechnology.com/servlet/…config -neutral&slug=TWGEIS&date=19991223 (last visited Oct. 14, 2001).
[30] See Mark Evans, Microsoft Burned by Hotmail Hackers, GLOBE & MAIL, Aug. 31, 1999, at A1, available at Westlaw, 08/31/1999 GLOBEMAIL A1.

crude as simply looking over a shoulder to observe the password being entered. Conversely, it may involve sophisticated software programs that allow the hacker to record the passwords of authorized users. Hackers may even possess valid passwords obtained through lawful means. For example, a hacker may be a former employee whose password has not yet been canceled.

Hackers, of course, do other things besides gaining access without authorization. They also send out viruses. These viruses may be designed simply to annoy, or may have considerably more sinister motives, perhaps the destruction of data.[31] Hackers may also engage in denial of service attacks. These activities make it difficult for legitimate users to access web sites, or preclude access altogether.

The computer has also created unique difficulties for law enforcement agencies regarding the storage and dissemination of child pornography.[32] Once again, the ubiquitous nature of the Internet has allowed for the dissemination of this type of material to an unparalleled degree. Similarly, the fact that national laws do not provide for a uniform set of rules creates an added layer of complexity. To make matters worse, the intention

[31] See Frontier, supra note 8 at 9 (presenting "Melissa" and "Explore.Zip.Worm" as examples of viruses that crashed systems and cost companies millions of dollars).

[32] See generally CYBERCRIME: Hearing Before a Subcommittee of the Committee on Appropriations, 106th Cong. 27 (2000) [hereinafter CYBERCRIME] (statement of Hon. Louis J. Freeh, Dir. of FBI, Dep't of Justice) Freeh states that the use of computers has made child pornography more available now then ever. The computer has enabled an offender "to transfer, manipulate, or even create…pornography." Id. Furthermore, the internet acts as a vehicle to transmit videotape or print media with improved processors and

to possess child pornography may be difficult to discern. Many pornographic web sites contain a number of catch phrases embedded in their HTML programming which are designed to draw visitors.[33] All users of the Internet will recall inadvertently visiting web sites other than those they had intended to visit. These sites frequently have a focus on sex.

Concomitant to the issues associated with child pornography are similar concerns related to the dissemination of hate material. Once again, a veritable patchwork of national legislation hampers any coordinated effort by law enforcement agencies. The country of Germany has gone so far as to pass laws which have been interpreted to be ostensibly extra-territorial in effect.[34] Under German Law, it is now an offence to disseminate hate material, whether or not the actual web server is located within Germany.[35] The German court, "the Bundesgerichtshof, issued a ruling . . . [in December 2000] . . . that overturned a lower court ruling and found that German [hate] law applies even to foreigners who post

modems. Id. Moreover, the ability to encrypt this data enables offenders to avoid detection. Id.

[33] See generally Maxim Kniazkov, File-sharing Allows Children Access Pornography on Internet, AGENCE FRANCE-PRESSE, Jun. 27, 2001, available at 2001 WL 24979408, at *2 (explaining how easy it is for children to gain access to pornographic websites). Filters are ineffective against file sharing programs. Id. In addition, pornographic websites may also contain links to child pornography sites. Id.

[34] See Angela Doland, French Challenge Yahoo! On Web Sale of Nazi Items, COMMERCIAL APPEAL, Jul. 25, 2000, at B10, available at 2000 WL 24140926, at *2.

[35] See Steve Kettmann, German Hate Law: No Denying It, WIRED NEWS, ¶ 2 (Dec. 15, 2000) (stating that the German law forbidding the dissemination of hate material, especially that which denies the existence of the Holocaust, applies to foreigners who post content on the web, which can be accessed inside

content on the Web in other countries, so long as that content can be accessed by people inside of Germany."[36] While the legal efficacy of the Court's ruling, at least insofar as it relates to foreigners, is dubious, it nonetheless sends a message to anyone who might try to distribute such material on the Internet.

The last issue identified under the rubric of computer misuse is the theft of information and theft of other analogous intangible items. Information and intangible rights are the foundation of our electronic borderless world. Their protection is essential to commercial society as it has evolved. Many of the activities do not constitute criminal theft per se, at least as such term has been historically defined in common law jurisdictions. A hacker's goal may be simply to gain access. His or her review of sensitive information contained in the penetrated web site may be a consequence of the activity undertaken, rather than an objective.

THE INADEQUACY OF EXISTING LAWS

Criminal law is, almost by definition in most Western jurisdictions, ill-equipped to deal with activities not contemplated at the time the rules were originally drafted. In addition to the maxim enunciated by the House of Lords in Shaw v. Director of Public Prosecutions that courts should be reticent to create new criminal laws[37], the criminal law is concerned primarily with tangible injury, either to the person or to

Germany) available at http://www.wired.com/news/politics/0,1283,40669,00.html.

[36] Id. at ¶ 2.

[37] See Shaw, [1962] A.C. at 241 (stating that creating new offences is "not within the province of the courts . . . [and] should be left to the legislature").

property.[38] Furthermore, the burden of proof resides with the state.[39] Thus, if there is no tangible injury, then a court will conclude, in the absence of explicit legislative direction, that no criminal activity has taken place.[40]

It should be made clear from the outset that many crimes committed with the assistance of a computer were already dealt with under existing criminal laws in most jurisdictions. Activities which could be construed as theft, fraud, forgery and mischief were already subject to criminal sanction.[41] However, all of these concepts have as their underpinning, measurable manifest harm, either to property or to the person.

Criminal prosecutors early on had difficulty applying common law principles to electronic media. The value of the electronic media is inherent in the information itself, rather than the media on which it is recorded. Theft of information may not cause any discernible harm to the vehicle it has been recorded upon. Nonetheless, the impact on the organization, which had its information stolen could be devastating. To illustrate this point,

[38] See 3 SIR JAMES FITZJAMES STEPHEN, A HISTORY OF THE CRIMINAL LAW OF ENGLAND 360 (London, MacMillen 1883).

[39] See Mark D. Rasch, THE INTERNET AND BUSINESS: A LAWYERS GUIDE TO THE EMERGING LEGAL ISSUES (Computer Law Association 1996) (explaining that criminal law imposes the burden of proof on the prosecution) reprinted in http://www.cla.org/RuhBook/chp11.htm, at 2 (Criminal Law and the Internet).

[40] See id. (explaining the prosecution's burden of proof). The traditional crimes provide inadequate analogues to computer crimes. Id. The criminal acts of computer criminals fall outside the scope of traditional crimes. Id. Without explicit criminal statutes that address computer crimes, the prosecution fails to prove each element of an analogues traditional crime beyond a reasonable doubt. Id.

[41] See The Phenomenon of Computer Crime, UNITED NATIONS MANUAL ON COMPUTER CRIMES, available at http://www.making-a-difference.org/computer-crime-chronicles.html (last visited September 25, 2001).

one writer gives the example of a former employee who accesses information from his former employer.[42] Must the information be "confidential" in nature to constitute property?[43] What if part or all of the information was publicly available?[44] Is knowledge on the part of the employee that the information is confidential relevant in determining whether or not a theft has taken place?[45]

The Canadian case of R. v. Stewart [46] addresses these questions. In Stewart, the defendant approached a hotel employee in an attempt to obtain copies of confidential records relating to the hotel's employees.[47] The purpose of obtaining the information was to assist in organizing a hotel employee union.[48] Mr. Stewart was charged, inter alia, with counseling to commit theft.[49] The case was considered by all three levels of the Canadian judicial system and garnered a wide variety of judicial opinions from the judges who considered the case.[50] A majority of the Canadian Supreme Court concluded that merely copying

[42] See Rasch, supra note 39, at 5 (describing the scenario in which "[a] former employee of ABC company, a defense contractor, now works for XYZ company, a competitor. His former employer has never deleted his computer account, and he accesses that computer to obtain valuable competitive bid information which he uses for the benefit of his new employer.").
[43] Id.
[44] See id.
[45] See id.
[46] [1988] 1 S.C.R. 963.
[47] See id at 966-967 (explaining that Wayne John Stewart offered a hotel security guard money for the names and addresses of the hotel's employees).
[48] See id. (explaining that Stewart assumed the union hired him). The union apparently sought the confidential employee information in an attempt to organize 600 hotel workers. Id. at 966.
[49] See id. (charging Stewart of unlawfully counseling "Jan William Hart to commit the indictable offense of theft, an offense as described in the Section 294 of the Criminal Code of Canada").
[50] R. v. Stewart, [1982] 38 O.R. (2d) 84 (S.C.(H.C.J.)), rev'd [1983] 42 O.R. (2d) 225 (C.A.), rev'd [1988] 1 S.C.R. 963 (Can.).

confidential information did not constitute theft.[51] The Canadian Supreme Court based its opinion upon the lower court decision which stated:

> that confidential information is not property for the purpose of the law of theft in Canada. . . . If this interpretation should be thought to be inadequate to meet the needs of modern Canadian society, particularly because of its implication for the computer age, the remedy must be a change in law by Parliament. It is not for a court to stretch the language used in a statute dealing with the criminal law, to solve problems outside the contemplation of the statute. If an accused person's conduct does not fall within the language used by Parliament, then no matter how reprehensible it may be, it ought not to be characterized as criminal.[52]

The view that information is not property is by no means a matter of unanimous legal thought, evidenced by the variety of opinions garnered in Stewart. That being said, the fact that jurists could conclude in the same manner as the majority of the Supreme Court of Canada invited legislative intervention in many jurisdictions.[53]

---

[51] See Stewart 1 S.C.R. at 972 (defining theft pursuant to § 283(1) of the Criminal Code of Canada). The court discusses how confidential information is not property as defined under § 283(1) nor should the court extend "the concept of property or . . . theft . . . under the Criminal Code." Id. at 979. Furthermore, the memorization or copying of confidential information is not an act which deprives the owner of possession or use. Id. at 980. The court concludes that confidential information lacks the essential quality of being tangible and therefore should not be considered property for the purposes of theft. Id. at 982-983.

[52] Regina v. Stewart [1983] 138 D.L.R. (3d) 73, 85.

[53] See Stewart at 1 S.C.R. at 979 ("To the extent that protection is warranted for confidential information, it should be granted through legislative enactment . . . .").

The issue of information as property is also raised, albeit somewhat tangentially, in the context of cases considering unauthorized access to computer networks.[54] Victims of unauthorized access often rely upon common law and statutory trespass laws to punish those who have gained entry without permission.[55] The difficultly inherent in this approach is that the law of trespass is fundamentally premised upon violations to real or personal property.[56] If the intrusion does not cause a measurable harm to the victim, then it may well follow that no trespass, from either a civil or criminal law perspective, has taken place.[57] Further, to exacerbate matters, criminal trespass laws often do not carry sanctions that are commensurate with the harm that might be inflicted by a cyber-trespasser.

Trespass may take a variety of forms in the Information Age. It may be constituted by unauthorized access to a computer

[54] See United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991) (discussing the unauthorized access requirement of 18 U.S.C. § 1030). See also America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 451 (E.D. Va. 1998) (stating that defendant's accessed AOL's computer network without authorization); Sawyer v. Dep't of the Air Force, 31 M.S.P.R. 193, 196 (1986) (stating that 18 U.S.C. § 1030 "defines as a criminal violation the knowing unauthorized access or use of the system for any unauthorized purpose.").

[55] See Benjamin Adida et al, The Future of Trespass and Property in Cyberspace (Dec. 10, 1998) [hereinafter Adida] (discussing the Common Law's limits in punishing unauthorized accessors to computer networks, as well as statutoty trespass laws that conflict with traditional understanding), available at http://cyber.law.harvard.edu/Itac98/final.html, at 3.

[56] See id. at 12 ("'Property' for trespass purposes is usually understood to be real property or chattel.").

[57] See id. at 4 (stating that the four elements of trespass are "(1)Intentional, (2)Entry, (3)Onto the property of another, (4)Without their express or implied permission to so enter" which does not take into account a victim's harm) (citing W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 13, at 70 (5th ed. 1984)).

network (i.e. hacking), spam e-mail or unauthorized access to a computer that is not networked.[58] It follows that a trespass analysis is not necessarily the same in the various scenarios.

Trespass can be civil or criminal in nature [59]; however, our focus is on the criminal aspects of trespass. The criminal laws related to trespass vary greatly, even within countries.[60] There are four elements that must be proven in order to establish criminal trespass. First, as with virtually all criminal offences, it is necessary to establish intent or mens rea.[61] In the real world, it may be difficult to assert that one is somewhere other than where they intended to be. That is not necessarily the case in cyberspace.[62]

In United States v. Morris [63], a computer science student devised a computer program called the Worm.[64] The Worm was designed to replicate itself on the computers that it contacted.[65]

---

[58] See id. at 3.
[59] Id. at 5.
[60] See Adida, supra note 55, at 5 (stating that there is no federal statute for trespass).
[61] See generally RONALD N. BOYCE & ROLLIN M. PERKINS, CRIMINAL LAW AND PROCEDURE 474-475 (7th ed. 1989) (explaining the requirement under criminal law of a guilty mind or intent).
[62] See Adida, supra note 55, at 7 (stating that in order to commit trespass, the trespasser must have "an intent to be at the place where the trespass allegedly occurred," which, in the context of cyberspace, means that the user of the computer accessing unauthorized information has the requisite intent to trespass via the computer).
[63] 928 F.2d. 504 (2d Cir. 1991).
[64] Id. at 505; see also F. LAWRENCE STREET & MARK P. GRANT, LAW OF THE INTERNET 664 (2000 ed. 1999) (discussing the Morris case and explaining that worms are a computer virus which replicate and fill a computer's memory) [hereinafter STREET & GRANT].
[65] See Morris, 928 F.2d at 506. Multiple copies of the worm would make it easier to detect and potentially cause the system to crash. Id. Morris designed the worm so that it would replicate itself only after the computer indicated that it did not replicate itself already. Id. Additionally, Morris wanted to prevent

Inadvertently, it did not detect that it had already infected a computer, thus causing it to continue replicating itself until the computer's memory was exhausted.[66] From a traditional mens rea analysis, a plausible defense to a criminal trespass action would be that Mr. Morris did not intend to trespass. Mr. Morris intended only for the Worm to simply enter a computer and replicate itself, without causing further harm. Such an argument could also be marshaled to rebut a charge of criminal mischief. However, the government successfully prosecuted Morris under the Computer Fraud and Abuse Act.[67]

The second element of criminal trespass is actual entry. [68] To enter physical property is usually self-evident. However, that is not the case in cyberspace. The California Court of Appeals considered this issue in Thrifty-Tel, Inc. v. Bezenek.[69] The Bezeneks' two children, Ryan and Gerry, accessed long distance

programmers from protecting their systems, therefore he created a default mechanism where the worm automatically replicated itself once after every seventh attempt to enter a computer. Id.

[66] See id. (stating that despite Morris' attempts, the worm created multiple copies of itself because Morris failed to anticipate the number of times a computer would allow the worm to enter). See also STREET & GRANT, supra note 64 and accompanying text.

[67] See Morris, 928 F.2d at 506 (stating that Morris was found guilty of violating 18 U.S.C. § 1030 (a)(5)(A)). See also STREET & GRANT, supra note 64, at 664-665 (discussing that in order to convict under the Computer Fraud and Abuse Act, the government need not show intent to harm, only intent to access without authorization); United States v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996) (holding that the only mens rea required to convict under 18 U.S.C. § 1030(a)(5)(A) is a showing of an intent to access without authorization). See generally 18 U.S.C. § 1030(a)(5)(A) (Supp. V 2000) (finding a person guilty of fraud in connection with computers if they "intentionally cause damage without authorization to a protected computer"); STREET & GRANT, supra note 64, at 661-663 (outlining the sections of 18 U.S.C. § 1030).

[68] See MODEL PENAL CODE § 221.2(2) (1962) (stating that criminal trespass is committed when a person enters upon property without authorization).

[69] 46 Cal. App. 4th 1559 (1996).

telephone numbers for which they would not be charged.[70] At first the children accessed the numbers manually and later used computer software.[71] The Court concluded that the electronic signals created by the boy's activities constituted trespass.[72] This analysis probably goes too far as it could logically extend to the simple act of someone looking over another's shoulder to view information on a computer screen. That conduct, although perhaps actionable on other grounds, cannot probably be regarded as trespass, at least premised upon any conventional view of the law.

The third element of a criminal trespass action is a finding of entry onto property.[73] We have already touched upon the position taken in R. v. Stewart that information is not property, which analysis would seem to preclude a Canadian criminal charge of trespass to information.[74] The definition of property varies greatly in trespass legislation. In American Computer Trust Leasing v. Jack Farrell Implement Co.,[75] a narrow definition of property was successfully argued to rebut an allegation of trespass.[76] The trespass allegedly occurred when the defendant's computer was wrongfully accessed to destroy

[70] Id. at 1563 (stating that the two teenagers used computer technology to access the telephone long-distance carrier codes to make free long-distance calls).
[71] Id. at 1564 (describing how the teenagers performed manual attempts to identify an authorization code through manual random searches, then expedited their process by obtaining computer software).
[72] See id. at 1566, n.6.
[73] See MODEL PENAL CODE , supra note, at § 221.2(2) (stating that a person commits criminal trespass when entering or remaining "in any place").
[74] See supra notes 46-51 and accompanying text.
[75] 763 F. Supp. 1473 (D. Minn. 1991).
[76] See id. at 1493-1494 (interpreting the Minnesota trespass statute not to include outside computer deactivation because the statute limits "trespass to

accounting and inventory records.[77] Citing the definition of property under Minnesota's trespass laws, the Court concluded that no trespass had taken place.[78]

A further complexity added to this rubric is that the aggrieved party must, in certain legislative regimes, be the property owner.[79] Given the plethora of intermediaries on the Internet, it may not be clear on whose property the perpetrator has actually trespassed. In fact, the aggrieved party may not be the actual owner.

The fourth and last element that must be proven to establish trespass concerns permission. If there is permission, be it express or implicit, then there is no trespass.[80] The use of spam, the sending of mass unsolicited e-mails, specifically raises the issue of implied consent. If an unsolicited letter is sent via regular post, there is generally no issue of the addressee not consenting to its receipt. However, the same logic does not necessarily apply to e-mail. The courts have generally concluded that the implied consent to receive unsolicited e-mails is limited. For example, in Cyber Promotions, Inc. v. America Online, Inc.,[81] the Court concluded that a sender of information did not have

things which are the product of the soil").

[77] Id. at 1493 (stating that defendant counterclaimed against ADP for allegedly destroying records).

[78] See id. at 1493-1494 (holding that accessing a computer was not in violation of Minnesota's trespass statute).

[79] See 75 AM. JUR. 2D Trespass § 39 (1991) (describing how in some jurisdictions it may be sufficient for the aggrieved party to establish it is the rightful user of the property).

[80] See id. at § 187 (stating that "the basic element of criminal trespass is unprivileged entry").

[81] 948 F. Supp. 436 (E.D. Pa. 1996) (affirming its November 4, 1996 decision).

permission to send a system debilitating number of e-mails.[82] Less than one year later, the Southern District of Ohio set a lower threshold by holding that spam constitutes trespass to an individual's email box.[83]

As a practical matter, the ability to send anonymous e-mail messages precludes effective law enforcement in this area. The response of the criminal law process to the possession and dissemination of child pornography obtained through the Internet is also quite murky. While the English Court of Appeals in R. v. Fellows[84] and R. v. Arnold[85] dismissed appeals brought by the perpetrators[86], a British Columbia trial court and the British Columbia Court of Appeal by placing paramount consideration on the liberty of the individual. The British Columbia Court determined that criminal legislation making it illegal to possess child pornography was unconstitutional.[87] Subsequently, the Supreme Court of Canada allowed an appeal and remitted the charges, finding that the prohibition of child pornography is

82 Id. at 456 (reasoning that because AOL's email servers use private property, the First Amendment precluded Cyber Promotions from littering AOL's system with mass advertisements).

83 See Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997) (reasoning that public interest is advanced by holding that high volumes of junk e-mail constitutes trespass to personal property because it congests Internet traffic causing e-mail recipients "to spend time and money wading through messages they do not want.").

84 [1997] 2 All E.R. 548-549.

85 Id.

86 See id. See generally 61 J. CRIM. L. 384-386 (1997) (providing commentary on the facts of the cases and the decisions of the courts).

87 See CBC-TV The National (CBC television broadcast, June 30, 1999)(transcript on file with The National Transcripts) (stating that the British Columbian Court of Appeal agreed with a lower court and found that possessing child pornography is not a crime) available at http://tv.cbc.ca/national/trans/T990630.html.

consistent with Canada's "charter values".[88]

In addition to the legal complexities encountered in pursuing criminal activities in cyberspace through traditional criminal laws, there is also a recognition that existing criminal laws may not provide sanctions that are commensurate with the damage inflicted. For example, Mafiaboy faced a fine of one thousand dollars (Canadian) for actions that inflicted millions of dollars in damages upon his victims.[89]

There is also a recognition that perpetrators locate themselves in jurisdictions where law enforcement is lacking or where no criminal laws exist to govern illegal computer activity. For example, the perpetrator of the Love Bug virus was located in the Philippines.[90] Under the law of the Philippines, it was not clear what crime was committed. Charges were initially contemplated under the Access Devices Regulation Act of 1998,[91] but that would appear to allow a potential defense that no secret information was obtained from other web sites. This legislation was enacted to make it a criminal offense to obtain credit card

[88] R. v. Sharpe, [2001] 1 S.C.R. 45, 175-176 (stating that "the benefits of the legislation far outweigh any harms to freedom of expression and the interests of privacy.").

[89] See Chaand & Streitfeld, supra note 15, at 3. Part of the difficulty in this case arises from the fact that Mafiaboy is a juvenile, and prosecutors have not sought to subject him to Canadian adult criminal law.

[90] See Philippine Officials Charge Alleged 'Love Bug' Virus Creator, (June 29, 2000) (describing how Onel de Guzman created a replicating computer virus that resulted in billions of dollars in damages, however, the Philippine government is having "trouble finding an applicable law to use since, until recently, the country had no laws against cyber crime.") available at http://www.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.html.

[91] Republic Act No. 8484, available at wysiwyg://171/http://www.chanrobles.com/republicactno8484.htm (last visited on Sept. 26, 2001).

and other personal information for a fraudulent purpose.[92]

Importantly, hacking *per se* does not appear to be a criminal activity under the penal laws of the Philippines.[93] This led to calls to extradite the alleged perpetrators to the United States of America for prosecution.[94] However, it is difficult to extradite a citizen to a foreign country for an activity not regarded as criminal in the domestic country. The extradition process is premised upon treaties that set out crimes an individual can be extradited for.[95] The 'Love Bug' case evidenced the need not just for domestic computer specific criminal laws in the Philippines, but also the need for a coordinated international effort.

THE LEGISLATIVE RESPONSES

The Scottish Law Commission issued a report in 1987 on

[92] See Raju Chebium, 'Love Bug' Suspect Could Face Both Civil and Criminal Trials, (May 8, 2000) (reporting that the law was initially written "to target credit card fraud but also covers the use of any unauthorized access device in order to obtain goods or services.") available at http://www5.cnn.com/2000/LAW/05/08/love.bug.02/index.html.

[93] See New Charges Urged in 'Love Bug' Case, (Sept. 5, 2000) (stating that the Philippines had no law against hacking as of the release of the 'love bug' virus) available at http://www8.cnn.com/2000/TECH/computing/09/05/erapa.virus/index.html. See also Revised Penal Code of the Philippines, Act No. 3815, (Dec. 8, 1930) (listing the crimes and penalties of the Philippines with no mention of computer hacking) available at www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm.

[94] See Suspected Hacker May Face Extradition Requests, (May 9, 2000) (stating that an extradition treaty between the United States and the Philippines could allow the creator of the 'Love Bug' virus to face charges in the United States) available at http://www.cnn.com/2000/LAW/05/09/internat.hacking.law.

[95] See John T. Soma et al., Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?, 34 HARV. J. ON LEGIS. 317, 323 (1997) (stating that "treaties are now required in order to allow for consistent and reliable extradition policies.").

Computer Crime and proposed the Computer Crime Bill.[96] The Bill highlighted the areas of greatest concern:

(1) Access to computer networks without authorization;

(2) What is meant by authorization;

(3) The law will apply if domestic data is affected, regardless of where the perpetrator is actually located.[97]

There was considerable debate as to whether unauthorized access to a computer network per se constituted a criminal activity.[98] Conceivably, a hacker could gain access to the network without the intention of causing harm. After leaving the network intact, the question arises as to what legal harm the perpetrator has caused. Based on a trespass analysis, the mere entry by the hacker would not be a civil wrong in most common law jurisdictions. However, it could perhaps be pursued as a criminal matter if the court was satisfied that the computer system was sufficiently analogous to real property. As discussed earlier though, this argument frequently presented prosecutors with an insurmountable barrier to obtaining a conviction.

The Data Protection Registrar in the United Kingdom took the view in the late 1980's that mere access to a computer network causing no damage was not a criminal act:

[96] See Scottish Law Commission Report, No. 174 (1987) (setting forth various computer crime offenses), available at http://www.underground-book.com/chapters/ccm/165.html.

[97] See id.

[98] Compare THE LAW COMMISSION, COMPUTER MISUSE, at 77-81 (Working Paper No. 110, 1988) (presenting arguments for making unauthorized access to a computer an offense) with id. at 81-82 (presenting arguments against making unauthorized access to a computer an offense).

> . . .juvenile 'hobby' behavior. The Registrar recognizes the undesirability of 'criminalising' juveniles and the concern that young people should not be introduced to the justice system unless necessary.[99]

Nonetheless, the consensus was that such activity presented real dangers to societies that were increasingly dependent upon computer networks.[100] Businesses were frequently put to considerable expense to ensure that the intruder had in fact caused no damage. Ultimately, the United Kingdom enacted the Computer Misuse Act 1990.[101]

The Act created a variety of offences, most of which were intended to address perceived inadequacies in the existing penal laws and their interpretation.[102] Referring to the relevant sections of the Act, the offences are as follows:

1 -unauthorised access to computer material;
2 -unauthorised access with intent to commit or facilitate commission of further offenses; and

---

99 IAN J. LLOYD, INFORMATION TECHNOLOGY LAW 182, (2d ed. 1997) (quoting from the Fifth Report of the Data Protection Registrar).

100 Id. at 183.

101 1990, c. 18 (Eng.), cited in Halsbury's Statutes of England and Wales, 1997 Reissue, Criminal Law, 1250 (vol. 12, 4th ed., Butterworths).

102 Andrew Charlesworth, Between Flesh and Sand: Rethinking the Computer Misuse Act 1990, 9 INT'L Y.B.L. COMP. & TECH. 31, 33 (1997) (stating that the Computer Misuse Act of 1990 created three new computer misuse criminal offenses). The author then explains that the three new offenses were "designed to avoid the type of problems that had come to light in the computer misuse cases that had already come before the courts." Id.

3 -unauthorised modification of computer material.[103]

This act utilizes the recommendations, which were proposed by the Scottish Law Commission's Report on Computer Misuse, by purporting to become extra-territorial in scope:

> It is immaterial for the purposes of any offence under section 1 or 3 . . . whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or whether the accused was in the home country concerned at the time of any such act or event.[104]

In particular, the Act sought to avoid the difficulties presented in earlier cases of proving actual damage in order to sustain a criminal conviction.[105] In Cox v. Riley[106], the English Court of Appeal considered the actions of the appellant who deliberately erased a computer program used to operate a saw.[107] Although the case itself turns on the interpretation of the Criminal Damage Act 1971[108], the nebulous discussion of the

[103] Computer Misuse Act, 1990, c.18 §§(1)(2)(3), at 1250, 1251, 1253.

[104] See id. § 4, at 1254.

[105] See id. § 3 (6), at 1253 (explaining damage under the Criminal Damage Act). A modification of the contents of a computer shall only be regarded as damage to the computer if the modification's effect on the computer impairs the computer's physical condition. Id.

[106] [1986] 83 Cr. App. R. 54.

[107] See id. at 55.

[108] See id. at 56 (explaining the parties' arguments). The defendant contended that the program was not property within the meaning of the Criminal Damage Act of 1971 section 10 (1). Id. See generally The Criminal Damage Act 1971, c.48, '(10)(1)(Eng.) cited in Halsbury's Statutes of England and Wales, Continuation Vol., 417 (vol.41, 3d.ed., Buttersworth, 1972) (describing the meaning of property and listing the section of the Criminal Damage Act of 1971 that describes the offense of destroying or damaging another's property).

Court concerned whether the erasure constituted damage.[109] The court also considered whether the determination of damage would allow future hackers and other computer wrongdoers to later assert that their actions did not cause tangible damage and therefore could not be prosecuted.[110]

The Computer Misuse Act 1990 has served as a model for many other countries' legislative initiatives on computer crime.[111] A few years later, Singapore passed the Computer Misuse Act 1993,[112] modeled after its U.K. predecessor.[113] Later in the decade, Malaysia in turn passed the Computer Crimes Act 1997[114], closely following the U.K. and Singapore models.[115] In

[109] See Cox, 83 Cr. App. R. at 56 (stating that the question before the court was whether the erasing of a computer program from a circuit card constituted damage within the Criminal Damage Act of 1971).
[110] See id. at 57-58 (dismissing the defendant's argument that erasing the computer program was not damage). The court notes that we are living in an age of computers and other magnetized operations. Id. at 56. From the court's holding it can be inferred that future hackers and other computer wrongdoers would not be able to claim that their actions did not cause tangible damage.
[111] See Soma, supra note 95, at 361 (stating that many countries within the Commonwealth Scheme used the Computer Misuse Act of 1990 as a model for their computer crime statute, such as "Great Britain, Australia, New Zealand, Canada, India, and the West Indies").
[112] 1993, c. 50a (Sing.) Lawnet, Home, Free Resources, Free Access Statutes, Legislation, #7 Computer Misuse Act (chapter 50a), http://www.lawnet.com.sg/free/vldb.htm (last visited Oct. 21, 2001).
[113] See Assafa Endeshaw, Computer Misuse Law in Singapore, 8 I.&C.T.L. 5 (1999). See also Moss City Court, Moss byrett, Norway, The Legal Framework – Unauthorized Access to Computer Systems, at *6, 11-12 (last updated Sept. 12, 2001) (e-mail from Stein Schjolberg to the Court) (outlining Singapore's Computer Misuse Act). See generally, Lim Siong Khee v Public Prosecutor, 2001-2 SLR 342; 2001 SLR LEXIS 69, at *6, 11-12 (High Court 2001) (finding the language of Singapore's statute similar to England's Computer Misuse Act of 1990).
[114] Computer Crimes Bill 1997, Malaysia, at http:www.mycert.mimos.my/crime.html (last visited Oct. 21, 2001).
[115] See Nagavalli Annamalai, Cyber Laws of Malaysia- The Multimedia Super Corridor, 12 J.I.B.L. 473-481 (1997). See also Moss City Court, supra note 113 at *21(outlining Malaysia's Computer Crimes Act 1997); Donna L. Beatty,

all, at least thirty-eight countries have been identified as having specific penal legislation governing computer access.[116] This list excludes India, which last year passed the Information Technology Act 2000.[117] Other countries have eschewed single purpose legislation, particularly those jurisdictions with codified criminal laws. In Canada, by way of example, Section 342.1 of its Criminal Code states:

> (1) Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system.
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) . . . in relation to data or a computer system, or
>
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable

Malaysia Computer Crimes Act 1997 Gets Tough On Cybercrime But Fails to Advance the Development of Cyberlaws, 7 PAC. RIM L. & POL'Y J. 351, 356-357 (1998)(stating that Malaysia's Computer Crimes Act 1997 was modeled after the UK's Computer Misuse Act 1990).

116 See Moss City Court, supra note 113 at *6 (listing 38 countries as having passed computer crime legislation as of Sept. 12, 2001).

117 See Indira Carr, India Joins the Cyber-race: Information Technology Act 2000, 2000 INT.T.L.R. 122 (2000) (explaining that India was slow in proposing computer crime legislation). See also Moss City Court, supra note 113 at *6, 18 (listing India, as of Sept. 12, 2001, as one of the countries, which has passed computer crime legislation and outlining the statute).

on summary conviction.[118]

The European Union has sought to present a unified approach for its member states with its proposed Draft Convention on Cyber-Crime (Draft Number 27).[119] The Convention deals with a variety of offences, including:

Article 2 - Illegal access;
Article 3 - Illegal interception;
Article 4 - Data interference;
Article 5 - System interference; and
Article 6 – Misuse of devices.[120]

The Preamble to the Convention recognizes the need for an internationally coordinated effort to combat computer crime.[121] In particular, the Internet is vulnerable to its weakest link. The presence of rogue or more lax jurisdictions will undoubtedly hamper law enforcement agencies operating in stricter regimes.

The need for the coordination of efforts is seen, even on a domestic level, within the United States of America. Computer

[118] Unauthorized Use of Computer of A Computer, R.S.C., ch. 27 § 342.1 (1) (1st Supp. 1985), amended by ch. 18, s. 18, 1997.
[119] Committee of Experts on Crime in Cyber-Space (PC-CY), European Committee on Crime Problems (CDPC), Draft Covention on Cyber-Crime, 50th Session, May 25, 2001, preamble, at *1 (recognizing a need to pursue a common criminal policy), at http://conventions.coe.int/treaty/EN/projects/cybercrime27.htm.
[120] PC-CY, ch.2, 1, supra note 119, at *3 (listing 6 "offenses against the confidentiality, integrity, and availability of computer data and systems"); Moss City Court, supra note 113, at *4.
[121] See PC-CY, preamble, supra note 119, at *2 (stating that computer crimes are criminal offenses at an international level and therefore require international cooperation).

crimes in the U.S. are first considered a state matter.[122] However, if it can be demonstrated that a federal interest is at stake or that the activity went beyond the confines of the state border, the activity will then also be regarded as a federal matter.[123] The State of Vermont was the last of the American states to pass computer crime legislation.[124] It is interesting to review Vermont's commentary concerning the desirability of passing specific computer crime legislation.[125] American legal scholars virtually beseeched Vermont legislators to pass such legislation[126], such as Gary Kessler, who notes that under Vermont law, the following were not criminal activities:

1. Destruction of program and data files;
2. Theft of program and data files;
3. Alteration of program and data files;
4. Depositing virus on backdoor programs; and
5. Denial-of-service.[127]

[122] Compare Sheri A. Dillon et al., Computer Crimes, 35 AM. CRIM. L. REV. 503, 507-08 (1998) (explaining that the first federal statute dealing with computer related crimes was passed in 1984) with id. at 529 (explaining that states began enacting statute dealing with computer related crimes in 1978). States considered computer crimes six years before the federal government. Id.
[123] Id. at 534 (explaining the conflict between state and federal laws). State statutes governing the theft or misuse of copyrightable material came into conflict with federal statutes because the federal government has exclusive jurisdiction over copyright law. Id.
[124] Julie A. Tower, Hacking Vermont's Computer Crime Statute, 25 VT. L. REV. 945, 945 (2001).
[125] See generally Gary C. Kessler, The Need for Computer Crime Legislation in Vermont, at *2 (1997) (explaining the importance of computer crime legislation in Vermont) at http://www.garykessler.net/library/crimeleg.html (updated July 2, 1999).
[126] See id. at *4 (arguing that Vermont needs to enact computer crime legislation and "join the rest of the country").
[127] Id. at *2.

As a practical matter, many computer crimes (and virtually all involving the Internet) have a Federal aspect to them. However, the writer's comments on the law in Vermont are limited to activities wholly within the state. The Computer Crimes Bill was finally passed into law on May 26, 1999.[128]

In the United Sates, the governing federal statute is the Computer Fraud and Abuse Act.[129] Originally passed in 1984, it has been amended four times, primarily to broaden its application.[130] The Computer Fraud and Abuse Act has seven substantive provisions, which are:

1030(a)(1) – "prohibits knowingly accessing a computer without authorization or in excess of one's authority and . . . accessing classified government information";

1030(a)(2) - "prohibits intentionally accessing a computer without authorization . . . and thereby obtaining . . . unclassified information";

1030(a)(3) - an absolute prohibition on accessing a government computer if that access affects its use (in essence a trespass provision);

1030(a)(4) – "prohibits knowingly . . . accessing a 'protected computer'";

1030(a)(5) - creates three classes of computer vandalism;

1030(a)(6) – "makes it a crime to traffic in passwords"; and

[128] Id. at *1.
[129] 18 U.S.C. § 1030 (Supp. IV 1999).
[130] Id. (stating that the statute was amended in 1986); 18 U.S.C. § 1030 (1994) (stating that the statute has been amended four times in 1986, 1988, 1989, and 1994).

1030(a)(7) – "prohibits communicating a threat to damage a 'protected computer'".[131]

It is interesting to note that the Computer Fraud and Abuse Act, in contrast to its U.K. counterpart, prohibits prosecution for the unauthorized access of a computer system where the object and thing obtained consists solely of the use of the computer.[132]

Having surveyed the legal environment that gave rise to the plethora of computer crime statutes, it is all but impossible to marshal an argument against legislative action in this area. In 1987, an author termed the musings of the Scottish Law Reform Commission on Computer Crime as "Scotch Mist".[133] However, given the exponential growth of the Internet, the concurrent growing dependence upon computers in our society, and the computer's obvious vulnerability to criminals, one doubts that such an article could be written today.

PUBLIC PERCEPTION

To what extent computer related crimes are properly viewed as being subject to criminal censure is a matter open for debate. It has been suggested that the activities of Mafiaboy produced a genuine sense of ambivalence on the part of many Canadians.[134]

---

[131] John M. Conley & Robert M. Byran, A Survey of Computer Crime Legislation in the United States, 8 INFO. & COMM. TECH. L. 35, 37-39 (1999). See also 18 U.S.C. § 1030(a)(1-7).

[132] Compare 18 U.S.C. § 1030(a)(4), with Computer Misuse Act, 1990, c.18, § 1(1), at 1253. See also Rasch, supra note 39, at 116.

[133] See Colin Tapper, "Computer Crime": Scotch Mist?, 1-72 CRIM. L. R. 4, 4-5 (1987) (considering the term "computer crime"). The author explains the Scottish Law Commission's skepticism of enacting computer crime statutes. Id at 22. Surveys do not evidence the need for computer crime legislation, and the author argues that doing nothing would provide the most flexible way of dealing with the issue. Id. at 8-9.

[134] See http://www.mafiaboy.com (providing links to more than 30 news articles discussing Mafiaboy) (last visited October 21, 2001).

There was almost a sneaking admiration for the Canadian teenager who brought certain large American Internet sites to a standstill.[135]

This public ambivalence was well demonstrated in R. v. Bedworth.[136] This case involved the activities of a University of Edinburgh student, who successfully hacked into the computer systems of the European Union and several banks in the United Kingdom.[137] In his defense, Mr. Bedworth asserted that his addiction to computer hacking precluded him from having the requisite intent needed to commit the offense of gaining unauthorized access, as described in the Computer Misuse Act 1990.[138] The jury agreed with this argument, acquitting Mr. Bedworth.[139] While the legal reasoning of the jury is suspect, it nonetheless demonstrates the view held by many in Western society: that hackers are not social pariahs.[140]

---

[135] Id. (showcasing websites which discuss Mafiaboy's youth, and painting him in the light of a cultural hero who was able to hack into major websites).

[136] Jim McClellan, Cyberspace: Married to the Monitor, OBSERVER, June 11, 1995, at 65, available at LEXIS, News Library (explaining that although the public was skeptical about granting Bedworth the defense of "computer addict", his lawyers felt that Bedworth's behavior justified the term addict).

[137] See Jonah McLeod, Let the Buyer Beware of Internet Commerce, INDUSTRY WEEK, May 1, 1995, at 58, available at LEXIS, News Library (discussing the need for skepticism when engaging in financial transactions on the network). The author uses the Edinburgh case as an example of a security hazard. Id.

[138] See Computer Hackers 'Broke Into Nasa', THE HERALD (Glasgow), May 21, 1993, available at LEXIS, News Library.

[139] See Jury Out on Trial Research: Recent Verdicts Have Sparked Concern, says Robert Rice, FINANCIAL TIMES (London), Aug. 6, 1996, available at LEXIS, News Library.

[140] See McClellan, supra note 136 (excusing Bedworth's conduct by describing it as an addiction like gambling). The article refers to Dr. Young's contact "center for on-line addiction". Id. See also http://www.netaddiction.com (last visited Oct. 21, 2001). Dr. Young works at the center for Online and Internet Addiction and provides "scientific validity" for internet addictions;

JUDICIAL CONSIDERATION OF COMPUTER CRIME LEGISLATION

There is now over ten years of judicial consideration of the Computer Misuse Act 1990 and sixteen years of American courts reviewing cases under the Computer Fraud and Abuse Act. The recent trend appears to be, to the extent possible, to a liberal and constructive interpretation of computer crime legislation.[141] The decision of the House of Lords in R. v. Bow Street Metropolitan Stipendiary Magistrate, ex. parte Government of the United States of America[142] (also known as Allison's case) is directly on point.

At issue in this case was whether or not an employee, who had access to certain data, could use that access to obtain data without the express authorization given by the employer.[143] The words of Lord Hobhouse leave no room for an accused to assert that, "Yes, I know that I was not authorized to access that data but I was authorized to access other data of the same kind."[144] Previous English decisions had cast some doubt as to what was meant by unauthorized access. In Director of Public Prosecutions v. Bignall and Another[145], the Court considered the activities of

http://www.netaddiction.com/services/legal/html (last visited October 21, 2001). "Dr. Young has testified in both state and federal courts." Id.

[141] Annual Rev. All E.R. 203, 204-205 (Butterworths London 2001) (explaining the expanding scope of the Computer Misuse Act of 1990). The House of Lords constructed the Computer Misuse Act of 1990 within the scope of pre-existing criminal laws. Id. at 205.

[142] [1999] 4 All E.R. 1, 1 (H.L.).

[143] Id. at 4.

[144] Id. at 7.

[145] [1998] 1 Crim. App. R. 1 (Q.B. Div'l Ct.).

two police officers.[146] The officers used access to the police computer for private gain.[147] The information was turned over by the police officers to a third party.[148] The Court held that the access was authorized, notwithstanding the fact that the access was used for an unauthorized purpose.[149] However, the decision in Allison's case makes it clear that authorization will now be construed against an employee who uses the information in a manner that was not intended by the employer.[150]

Interestingly, many of the reported cases involving the interpretation of computer crime legislation concern disputes between employers and former employees.[151] Although the original rationale for these laws was societal dependence upon the computer, the reality is that computer crime laws are now being used primarily as weapons in what are ostensibly civil disputes. In Shurgard Storage Centers v. Safeguard Self Storage,[152] the U.S. Federal District Court considered the application of the Computer Fraud and Abuse Act to a dispute

[146] Id. at 1-2.
[147] Id. at 1.
[148] Id. at 2.

[149] See id. at 12. See also Halsbury's Laws of England, Annual Abridgment 1997, 262, § 933 (Butterworths 1998) (explaining that the court deemed the officer's access as authorized due to the primary purpose of the Computer Misuse Act of 1990). The court further stated that the primary purpose of the act is to "protect the integrity of the computer systems and not the integrity of the data stored on them." 1 Crim. App. R. at 1.

[150] See Allison's Case, supra note 142, at 10.

[151] See Edmond B. (Peter) Burke, The Expanding Importance of the Computer Fraud and Abuse Act, at, *1, *4, available at http://www.gigalaw.com/articles/2001/burke-2001-01-p1.html (last visited October 21, 2001) (explaining the significance of the Computer Fraud and Abuse Act in the departing employee/employer context).

[152] Id. at *3 (citing the Shurgard case).

between an employer and a disloyal former employee.[153]

In Shurgard, the employee obtained access to information within the ambit of the express authorization granted to him by his employer.[154] This information was then taken with him when he left to join a competitive firm.[155] The plaintiff argued that the employee had accessed the computer without authorization, thereby violating the Act.[156] Implicit in any authorization is a limitation on how the information will be used. The Court agreed with the plaintiff's submissions, stating "that the authority of the plaintiff's former employees ended when [he] allegedly became agents of the defendant."[157] This approach follows the narrow view of authorization taken by the House of Lords in Allison's case.

The extent to which "civil" disputes apply "criminal" computer crime legislation was recently demonstrated when a Singapore employer brought suit against its former employees. Two lawyers were charged under the Computer Misuse Act 1993 with copying computer data after they tendered their resignations from their law firm.[158] Interestingly, the information which was copied relates solely to precedents. There appear to be two conflicting approaches that might be taken by the court in this case. Firstly, one may argue that once the employee's

[153] Id. at *4.
[154] See id.
[155] See id.
[156] See Burke, supra note 151, at *5.
[157] Id.
[158] Lawyers Charged with Copying Data, STRAITS TIMES (Sing.), Jan. 17, 2001, at 1 available at LEXIS, News Library, also available at 2001 WL 4936290 (reporting that the charges were laid on January 17, 2001).

resignations were tendered, then their authorization to copy the computer material ended. Conversely though, it can be argued that the copying of precedents, as opposed to client information, was well within the express authorization of their access. In any event, it is apparent that computer crime legislation is once again being used as a weapon in civil disputes.

Yet the passage and implementation of computer crime legislation has been no panacea. There remains the need for a coordinated international effort, particularly as the activities relate to the Internet. For example, the author of the Love Bug virus was not subject to criminal censure as the result of outdated penal laws in the Philippines.[159] As a practical matter, many of the authors of recent viruses are outside criminal prosecution.[160] Similarly, proving authorship of a virus program or denial of service attack can be very difficult. Therefore, evidentiary issues are invariably problematic in pursuing such crimes.

Difficulties in prosecutions have also arisen as consequence of the actions of the victims themselves. Many businesses are loathe to publicly admit a breach of their computer networks. Such an admission may be commercially damaging and serve as

[159] See Grace D. Sarmiento, Philippines: NBI Reopening Love Bug Case, COMPUTERWORLD PHILIPPINES, June 18, 2001, available at 2001 WL 8187704 (explaining that two months after the charges were filed against the 'Love Bug' perpetrator, the charges were dimissed after a court found the offense could not be punished under RA 8484). See also, South China Morning Post Ltd., Cyber Laws Needed for Virtual Crime, MORNING POST (China), May 18, 2000, at 14, available at LEXIS, News Library (explaining that the Philippine authorities struggled to find grounds on which to charge the 'Love Bug' perpetrator since computer hacking was not a crime in the Philippines); supra notes 90-95 and accompanying text.

[160] See Charlesworth, supra note 102, at 39 (stating that "the authors of

an invitation for further attacks to other computer criminals.[161] That being said, it is submitted that the lack of prosecution by a victim does not undercut the necessity for computer crime legislation.

CONCLUSION

The need for specific computer crime legislation was manifest in most jurisdictions, however, prosecutors have faced a number of difficulties in applying existing criminal laws. In part, this challenge related to the systemic bias in favor of the accused. An additional challenge was the criminal law's fixation on the tangible and its inability to adapt to technological change.

Laws that existed prior to the passage of specific computer crime legislation were wholly inadequate. Prior to legislative intervention, what was literally described as "open season" in the state of Vermont, there were significant problems with conventional legal analysis. Allegations of trespass against computer hackers were fraught with a number of problems.[162] However, computer crime legislation avoids such problematic arguments, like the arguments that damage was not done to property. As well, it avoids any technical argument that the mere access was not trespass and therefore not actionable.

Furthermore, previous criminal laws frequently did not carry sanctions that were commensurate with the harm inflicted. Society's notion, that the hacker is an anti-hero is ebbing; due to the fact that as businesses and the public recognize the tangible

many prevalent viruses are effectively beyond the arm of the law").

[161] See Dillon, supra note 122, at 505 n.8.

[162] See Adida, supra note 55, at 121 and accompanying text.

harm that these wrongdoers can inflict. Specific legislation resolves ambiguities and allows for penalties that are appropriate. Also, specific computer laws avoid complex issues of intent, where the intent of the villain may be something less than the harm inflicted.

Ultimately the most persuasive argument that can be brought favoring specific computer crime legislation is for the evolution of our information society. Businesses and societies have become immensely dependent upon the information infrastructure. Great value is now rightly ascribed to the intangible.

The enactment of the Computer Misuse "Acts" in various jurisdictions as well as the Computer Fraud and Abuse Act in the United States represent necessary legislative interventions to address actual and manifest inadequacies in the criminal law. The extent to which this intervention was required cannot be assessed with mathematical precision. What can be said however, is that it was clear that the existing criminal laws in many jurisdictions were entirely ill-suited to deal with the myriad of issues.

The computer remains the cornerstone device used in the accessing and processing of information. Developed commercial societies cannot afford to sit idly by in the hopes that ambiguous and often outdated laws can be reshaped to redress wrongs that were not contemplated by the original law's drafters. The drafting, implementation and eventual amendments to computer crime legislation, represent an essential response to a social imperative arising in the Information Age.