11

Canada's computer crime laws: Ten years of experience

Martin P.J. Kratz
Bennett Jones Verchere
1000, 10035 - 105 Street, Edmonton, Alberta Canada T6M 2K4
403 421 8133, fax 402 421 7951, email mkratz@ccinet.ab.ca

Abstract

The role of the criminal law is to act as a deterent to conduct considered so damaging that the intervention of the state is warranted. Increasingly computer security issues have sought to use the power of criminal sanctions to deter abusive behaviour. This the approach taken by Canada. An additional set of civil and quasi-criminal remedies is also available under Copyright law. The paper reviews Canada's experience with both the criminal and copyright sanctions in the context of computer abusive behaviour including that carried out through use of the internet. The importance of an effective computer use policy is emphasized throughout.

Keywords

Computer crime, computer abuse, software piracy, telecommunications abuse or misuse, criminal law, copyright law, theft, fraud, computer use policy, computer abuse task force

1 INTRODUCTION

The purpose of this paper is to provide an overview of Canada's computer crime laws under the Criminal Code of Canada, R.S.C. 1985, Ch. C-46, as amended and the quasi-criminal sanctions under the Copyright Act, R.S.C. 1985, Ch. C-42, as amended, which may provide a basis for prosecuting or deterring some forms of computer abuse. Canada's computer crime laws were proclaimed law in December 1985 and since that time society has seen several new types of antisocial behaviour including creation and release of computer viruses and a variety of misconduct relating to use of the internet and other networks.

Given the changing nature of some forms of abusive conduct it is important to examine the extent the existing law still provides adequate sanctions to deter such conduct.

Under Canadian law generally, no criminal offence exists unless it can be found within the Criminal Code. This simplifies and clarifies the citizens' obligations and the state's possible actions against persons committing alleged criminal conduct.

This paper will outline the key features of Canada's computer crime laws and detail some of the cases which have interpreted these laws to date. This background and the detailed

S. K. Katsikas et al. (eds.), *Information Systems Security*

commentary contained herein should assist those persons interested in security of computer systems, both in Canada and elsewhere and in using the legal tools in fashioning more secure computer systems. In particular an understanding of the criminal sanctions emphasizes the need for organizational computer and software access and use policies to be implemented and enforced.

2 BACKGROUND OF COMPUTER CRIME LAWS

Criminal law in Canada is a matter for federal jurisdiction and therefore the criminal law is uniform throughout the country. Similarly copyright law is also within the exclusive jurisdiction of the Federal Government.

As a result in Canada and unlike the situation in the United States the same criminal law applies equally to all computer systems, data and software regardless of who the owner is, regardless of which province the offence occured in and regardless of whether the offence crosses provincial boundries. By contrast in the Unitied States each state imposes its own criminal law often with differences between states. Overlaid on this framework are different provisions applying to criminal conduct over which the U.S. Federal government has jurisdiction, interstate offences and offences relating to federal interest systems.

Traditionally many types of criminal conduct may involve computer programs, storage media or data but that are not what is commonly thought of as "computer crime". For example, theft of a system unit or other hardware component is merely theft of a particular physical asset. There is nothing mysterious or unusual about such criminal conduct and the criminal law has a wealth of experience in dealing with that type of criminal activity. The purpose of this paper is not to examine this type of activity.

There are certain types of conduct which have provided difficulty for the established framework of criminal law. Data and computer programs are ephemeral. Considerable damage may be done merely by using or accessing a computer system or by destroying or altering data. Since many of these concepts are new to the criminal justice system, many jurisdictions have found it necessary to enact new, specific, computer crime laws. The purpose of this paper, then, is to examine these specific computer crime laws and certain of the general laws which deal with other nontraditional applications for criminal law in relation to the computer industry.

There are several major categories of computer crime, as defined above. These are:

1. Unauthorized use of a computer system or computer services;
2. Unauthorized use or reproduction of computer programs;
3. Unauthorized use or reproduction of data;
4. Theft of computer system hardware, programs or data or the information contained therein;
5. The commission of other offenses (such as theft of other physical assets or destruction of assets) through use of the computer as the medium for committing the offence; or
6. Denial of or interference in the access by legitimate users of a computer system, computer services, computer programs or data whether by release of computer viruses or other means.

The particular characteristics in respect of many of the types of computer crime make this area of criminal law particularly difficult for the professional investigator or law enforcement official. Some of these peculiarities are as follows:

- Many computer crimes are undetected. Often use of a computer as the medium by which a particular offence is committed leaves no trail of evidence through which the conduct can be detected. Often it is the discovery of some incidental byproduct or activity related to the criminal conduct which results in discovery of the offence (i.e. sudden wealth).
- A wide range of assets are available through their representation as data stored in a computer system. Money, monies worth, inventory, and other property may be recorded or represented by data in various computer systems. The ease of manipulation of this data provides the computer criminal with relative ease in manipulating the underlying assets.
- There is a wide geographical area in which computer crime occurs. Through the use of telecommunications access, it is possible for a criminal to institute a chain of events in one jurisdiction, say, in Greece, which results in loss or injury in another jurisdiction, say Ottawa, Canada. There are problems of which law, if any, would apply to this particular criminal conduct. Furthermore, there is an additional difficulty of extradition which would complicate prosecution.
- There are innumerable points of access from which the particular abusive conduct may occur. Through the interconnection of many computer systems in local area networks, wide area networks or otherwise through telecommunication channels, there are a multiplicity of points of access from which the criminal activity can be initiated.
- The relative informality of users and many system operators on the internet make it difficult to introduce meaningful security. This coupled with the increasing transaction of business on the Internet create a wealth of opportunities for a variety of criminal conduct.
- A contracted time scale may be involved. In many types of traditional crime the criminal conduct may take minutes or even hours to commit. In some cases it may take days or months to commit certain types of crimes. Data or computer programs can be erased, manipulated or altered in seconds.
- The range of assets available to the computer criminal is less limited. A few key strokes may allow the diversion of a significant amount of inventory from a warehouse. A traditional fraud or bank job may deal only with the physical assets which are directly available to the criminal or the victim. The computer and telecommunications system provide a broader range of access to the victim's resources for the computer criminal.
- Software piracy is extremely widespread. The "sharing" of computer programs provide a vector for the transmission of computer virus programs and significantly enlarges the class of potential victims of the abusive conduct.
- Access to and use of the internet is very widespread. Downloading of computer programs or other files may provide a vector for the transmission of computer virus programs and significantly enlarges the class of potential victims of the abusive conduct. Furthermore the informal way in which many users do business, provide private information or data on the internet leads to wide dissemination of vulnerable data, such as credit card numbers, confidential telephone numbers, calling card numbers, passwords or other imbedded information. The availability of such sensitive information provides more opportunities for opportunistic criminal activity.

- To the extent that computer security systems are in place, they are often and commonly subverted by the users of the systems who select easily defeated passwords or otherwise compromise the system security on the basis of maximizing user convenience.
- It is the widespread proliferation of intelligent devices, such as laser printers, facsimile transmission machines and the like which expand the range of entry points for corruption of a computer, network or telecommunications system.

There are a number of initial matters which must be considered and reviewed prior to an in depth analysis of the Canadian experience with enactment of specific computer crime laws.

These preliminary matters, are, first, the fact that most computer crime laws are based upon the concept of authorization or "colour of right" in respect of the use of computer systems, programs or data, and, second, the fact that there are particular problems in admissibility of computer generated records. These matters are discussed below.

3 AUTHORIZED USE AND A COMPUTER USE POLICY

Computer crime laws dealing with unauthorized use of computer systems, computer programs or data are premised, fundamentally, on the concept that there is an approved range of permissible activity in relation to the system, programs or data. Unfortunately in many large (or small) computer installations there is no computer use policy. Similarly few web site or home page operators on the internet set out the rules for use of their system.

This causes significant difficulty for the prosecutor who must then show that the particular conduct complained of was not authorized by the owner or operator of the computer system. While unauthorized use is easier to show in respect of an outsider gaining access to an internal or proprietary computer system, it is a particularly difficult problem when dealing with an insider (i.e. employee or consultant) who has, on a routine base, access to the computer system, programs and data or when dealing with an open network such as the internet where external access to the computer system is encouraged.

It is strongly recommended that any system operator or owner of any computer system establish a thorough computer use policy.

It is also recommended that the system operator or owner also establish a computer abuse task force consisting of, at least, a representative of management with the authority to make decisions about an investigation (who may also have authority to take action based on the results of the investigation or who may report to senior management), an attorney with experience in computer law matters, and an outside computer consultant who may provide an external means of assessing the abuse and analyzing the fact situation underlying the abuse, so as to establish the mode of the abuse, the identify of the abuser(s), and such other information as may be useful in subsequent prosecution.

The computer use policy is a very important ingredient in any effort to control potential computer abuse. As a result, it is important that such a policy be well thought out and reflect the actual working environment of the particular computer systems, programs and data. Artificial rules which are routinely broken will not provide the security that is desired from such a computer use policy. Therefore in addition to the policy being meaningful, the system operator or owner must also:

- Communicate that computer use policy to all persons who may have access to or use the computer system, programs or data; and
- Be prepared to take enforcement action to ensure compliance with the computer use policy.

4 LEGISLATIVE PROVISIONS IN THE CRIMINAL CODE OF CANADA

There are five (5) main areas of criminal law which are relevant to many cases of computer abuse in Canada. The appropriate legislative provisions are cited below and certain relevant or significant commentary is provided after each provision.

4.1 Unauthorized Use of a Computer System

Section 342.1 states:

(1) Everyone 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, computer system with an intent to commit an offence under (a) or (b) or an offence under Section 430 in relation to data or a computer system

is guilty of an indictable offence and is liable to imprisonment for a term not exceeding 10 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 function;

"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 abnormal 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."*

The essence of the offence is the fraudulent obtaining of a computer service without authority or colour of right or intent to use a computer system to create one of the mischief offenses (Section 430).

In the context of the internet the offence may be committed by using a "sniffer" to identify other person's passwords and accounts and gain access to the internet thereby. Similarly it would appear to be clear that the offence is committed by breaking though a firewall and entering into the private system behind the firewall.

There have been a number of Canadian convictions under this section but are as of yet no reported case law dealing with the meaning or effectiveness of this provision.

In the absence of specific judicial commentary in Canada on this provision, it may be useful to note a number of prosecutions under similar legislation in other jurisdictions. In U.S. v. Sampson (1978) 6 CLSR 879 (ND CALIF) the defendant was able to obtain telecommunications access to a U.S. government computer system. The court held that the defendant had no intention to pay for such use. The defendant was charged under 18 USC 641, which deals with the embezzlement, theft, or conversion of records or other things of value belonging to another. The case proceeded on the basis that the defendant stole "things", being computer time and storage capacity to the value of $1,924.00. The defence argued that the computer time and computer storage capability were not "things of value" within the meaning of the legislation. At page 880, Ingram, D.C.J., held:

> "Consumption of its time and the utilization of its capabilities seem to the Court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be doubted. Thus, the uses of the computer and the product of such uses would appear to the Court to be a 'thing of value' within the meaning of 18 USC 641, sufficient upon which to predicate a legally sufficient indictment."

This interpretation has been criticized by Brown, "Crime in Computers" (1983) 7 CRIM LJ 68, as being a strained interpretation of the enactment.

4.2 Mischief in Relation to Data

Subsection 430 (1.1) states:

"Everyone 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, interrupts 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."

Subsection (5) provides that this provision is also a hybrid offence carrying a maximum term of imprisonment on conviction of the indictable offence of five years. Subsection (8) provides that "data" has the same meaning as in Section 342.1.

In Re Turner v. The Queen (1984) 13 C.C.C. (3d) 430 (Ontario High Court) the Court held that the unauthorized encrypting of data on magnetic tapes in a manner such that the data could not be properly accessed or used by the owners of the data could constitute an offence under the general mischief provision. This was basically a recognition that the offence deals with the ability to enjoy the use of property rather than any physical interference or modification of the property itself. The Court specifically noted the provisions of Subsection 430 (1.1) above, which were, at that time, before Parliament but not yet enacted into law. The judge noted that the conduct of the defendant in encrypting data and thereby essentially destroying the access to that data by the legitimate owners of the data, could also fall within the (then) draft Section 430(1.1)).

A very current problem is that of computer virus contamination. A computer virus program is a computer program with a reproductive strategy as well as carrying a logic bomb of some kind. The nature of operation of computer virus program is, generally, to attach itself to an existing computer program. If attachment occurs to sufficiently many computer programs then the memory space in the computer system can be substantially reduced. It would appear that such attachment alone would constitute an alteration of data within the meaning of 430 (1.1) (a) and in some cases may obstruct, interrupt or interfere with the lawful use of the data under Subsection 430 (1.1) (c). There have been numerous convictions in Canada under this provision for a variety of acts including using a programmed modem to call all computers in town seeking to identify system and release of virus programs on the internet.

When the logic bomb of a computer virus program is triggered it can carry out a wide range of activities from harmless messages to instruction of data files, computer programs or worse. This is the result whether the rogue program was acquired on the internet or through some other means. Such activity also appears to fall within the meaning the Section 387 (1.1) (a), (b), (c) or (d) in the appropriate circumstances.

4.3 General Theft Provision: (Theft of Confidential Information)

Section 322 states:

"(1) Everyone 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 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."

The key issue has been whether or not there is property in confidential information since the provision, above, is based upon a property construct.

The root case on the use of this provision in respect to the theft of confidential information or data is R. v. Stewart (1982) 68 C.C.C. (2d) 305, 38 O.R. (2d) 84 (Ontario High Court), reversed by (1983) 42 O.R. (2d) 225, 5 C.C.C. (3d) 481 (Ontario High Court of Appeal) reversed, (1988) 1 S.C.R. 963, Supreme Court of Canada. In this case a computer consultant attempted to acquire confidential employee data from a hotel's computerized data base so as to provide a union wishing to organize the employees of the hotel with information on the identity and address of employees. The union had asked for this information and been refused.

The majority of the Ontario Court of Appeal held that since valuable confidential business information was treated as a form of quasi-property by the civil law, then this was sufficient for it to constitute property for the purposes of the Criminal Code and therefore the offence of theft of confidential information could lie. The Supreme Court of Canada reversed and overturned the Ontario Court of Appeal's decision.

In the Supreme Court of Canada, Justice Lamer, writing on behalf of the other five judges in the Stewart case, held that confidential information that is copied or memorized in a covert manner cannot be considered property which is capable of being stolen. The primary basis for this decision was the deprivation theory, if one takes my information I still have the information so I have not been deprived of any thing. Justice Lamer balanced society's interests and held that society's interest in the free flow of all sorts of information had a priority over the injury suffered by a victim whose valuable confidential information is misappropriated. Justice Lamer drew analogy between information generally and the air we all breath. He said "no conviction for theft would arise out of a taking or converting of the air that we breath, because air is not property."

In providing the kernel of his decision based on a deprivation theory, Justice Lamer said, "one cannot be deprived of confidentiality, because one cannot own confidentiality. One enjoys it."

In balancing the interests of society and the victim of misappropriation of valuable confidential information, the court looked to some extreme examples. For example, Justice Lamer said, "Would society be willing to prosecute the person who discloses to the public a cure for cancer, although its discoverer wanted to keep it secret?" With respect this type of philosophy strikes to the very heart of modern commercial enterprises, in particular high technology industries.

It is vital, however, that one understand that the Supreme Court's decision in the Stewart case is not legally perverse. Rather, the decision of the Supreme Court of Canada follows a long and well established legal tradition in dealing with the problem of protection of information using property concepts. This legal tradition has not been able to adapt sufficiently to the special needs and incredibly rapid growth and development of the advanced technology industries. It is important to have a better understanding of this traditional legal approach so that effort may be focused on law reform efforts. In the Stewart case, Justice Lamer noted that it was the proper place of the legislative authority to make major changes in the operation or scope of the criminal justice system and not the place of the courts to do so.

The criminal law is inevitably based upon its historical roots. Criminal law in the Anglo-American tradition are fundamentally built upon property concepts and dealings with animate objects. As a result, there has been significant controversy in the area of unauthorized access and use of confidential information. A number of cases have focused on the issue of whether confidential information can be characterized as property. Generally the view throughout the Commonwealth is that confidential information is not property within the conventional meaning of the term property. In Malone v. Metropolitan Police Commissioner [1979] 2 WL 700 (Ch. D) the Court held that the electrical impulses constituting a confidential telephone conversation were not property. In Oxford v. Moss [1979] CRIM LR 119 (DC), the Court held that confidential information contained in an examination paper was not property. Legal commentators utilizing traditional concepts and approaches view the potential for a concept of "theft" of confidential information as disturbing. R.J. Roberts, "Information Property", (1987) 3 IPJ 209; R.A. Brown, "Computer Related Crime Under Commonwealth Law, In the Draft Federal Criminal Code", (1986) 10 CRIM LJ 376; and C.C. Ruby, "Annotation" 51 CR (3rd) 378. Notwithstanding this conservative approach, some courts such as the majority of the Ontario Court of Appeal in the Stewart case continue to attempt to provide meaning for the criminal law in a modern age when legislative reform consistently is outpaced by technological development.

Jurisprudential conservatives argue that there is no role for the judiciary in carrying out such a legislative role. There are many good points to be made for this perspective, including the fact that the results of one judicial decision can have widespread effect without the benefit of the public debate which normally accompanies legislative reform. However, on the other hand, the courts have not been reticent in developing other areas of law to adapt to technological change. As a result, significant interests in society may be protected. For example, in Canada, judicial decisions had, for several years prior to enactment of specific amendments to the Copyright law, established that computer programs are literary works within the meaning of the Copyright Act. As a result, a stable foundation has been provided for the Canadian industry developing, using and dealing in computer programs.

Law reform in Canada generally takes some considerable time. A Federal - Provincial working party on trade secrets has recommended reform of both civil and criminal law of trade secrets. Dealing with criminal misappropriation of trade secrets, the report recommends the creation of several new criminal offenses which would deal with "misappropriation of trade secrets" (Section 301.3) and "fraudulent misappropriation" (Section 338.1). These Sections are, at this stage, merely recommendations. The Sections are quoted below.

Section 301.3 (Misappropriation of trade secrets)

"(1) Everyone who fraudulently and without colour of right acquires, discloses or uses the trade secret of another person, without the consent of that person, within intent to deprive that other person

(a) Of control of the trade secret, or
(b) Of an economic advantage associated with the trade secret

is guilty of an indictable offence and is liable to imprisonment for ten years, or of an offence punishable on summary conviction."

Section 338.1 (Fraudulent misappropriation)

"Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of the Act, induces any person to disclose, or to permit another person to disclose or use, a trade secret, is guilty of an indictable offence and is liable to imprisonment for ten years, or of an offence punishable on summary conviction.

The definition for trade secret is proposed to contain five elements. Thus a trade secret is:

(a) Information that;
(b) Can be used in a trade or business;
(c) Is not generally known in the trade or business;
(d) Has economic value from not being generally known; and
(e) Is the subject of reasonable efforts to maintain its secrecy.

It still remains to be seen whether or not these proposed reforms will be considered by Parliament in reforming the Criminal Code of Canada. Obviously Parliament will have to balance the need to deter industrial espionage with the necessary safeguards to prevent the criminalization of many types of civil behaviour.

As discussed earlier in this paper, the theft provision provides a meaningful and workable remedy for dealing with misappropriation of computer hardware or physical diskettes or other media upon which computer programs or data are stored. As will be discussed below, the Copyright Act provides some limited ability to deal with unauthorized reproduction of computer programs or data.

4.4 Theft of a Telecommunication Service

Section 326 states:

"(1) Everyone commits theft who fraudulently, maliciously, or without colour 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 327, "telecommunication" means any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system."

In R. v. McLaughlin (1980) 53 C.C.C. (2d) 417, (1980) 2 S.C.R. 331, 18 C.R. (3d) 399, the Supreme Court of Canada held that the unauthorized use and alteration of programs and data at the University of Alberta computing facility did not involve the use of any telecommunication facility within the meaning of Section 287 and therefore no offence was committed. The University of Alberta, like many large computer installations, has many

remote access terminals which use telecommunications means to effect communication between the remote terminal and the mainframe computer. It is noteworthy that in this case a remote terminal was used. The Supreme Court of Canada, however, took the broader view and characterized the entire installation as computer facility and did not focus on the telecommunications aspects of the access.

Either Section 342.1 (unauthorized use of a computer system) or Section 430 (1.1) (mischief in relation to data) would now be the provision under which this type of offence might be charged.

In R. v. Miller (1984) 12 CCC (3rd) 466 (Alta CA), the court examined Section 326 (1) in a case dealing with unauthorized interception of cable television transmissions. The defendants were subscribers to cable television service for which they paid. In addition they also received a descrambled pay T.V. channel for which they did not subscribe. Upon the evidence of the defendants, which was accepted by the court, the pay television channel was received in black and white and not scrambled. The defendant alleged he had problems with cable reception and devised a "tuneable stub" consisting of a length of coaxial cable and some tin foil which he attached to his television set. The court accepted the evidence of the defendant's that the use of this "tuneable stub" corrected the reception problem with his regular cable reception. A side benefit of the use of this "tuneable stub" was the fact that it allowed reception in an unscrambled form and in full colour of the pay T.V. channel which the defendants then proceeded to enjoy without making payment. The court argued that for a conviction to lie, the obtaining of the service must be fraudulent, meaning the act must be intentional, under no mistake and with the knowledge that the goods were the property of another. In this case the court found that the defendants had received the unscrambled signals through no connivance of their own and therefore the mere watching of those signals was not an offence under Section 326 (1)(b).

In the Miller case, expert evidence was lead to disprove the defendant's story of poor cable reception. However, the court found in favour of the evidence given by the defendant's expert witness. As a result, in a case under this Section or for that matter under any provision in the Criminal Code, the prosecutor must be sure to provide the highest quality of credible expert evidence in support of their case as is possible.

In other jurisdictions without similar legislation, prosecutions for unauthorized use of telecommunication services has proceeded upon different legal theories. In Australia, for example, prosecutions in this area have initially been developed by recourse to the concept of theft of electricity. Scottings & Rasjke [1957] CRIM LR 421; Low v. Blease [1975] CRIM LR 513 (DC).

Related to the offence of theft of a telecommunication service is Section 327 which deals with possession of a device to obtain a telecommunications facility or service without payment of a lawful charge. Subsection 2 provides for forfeiture of the device and Subsection 3 provides for limitations on such forfeiture.

Section 327 states:

"Everyone who, without lawful excuse, the proof of which lies upon him, manufacturers, possesses, sells or offers for sale or distribution any instrument or device or any component thereof, the design of which renders it primarily useful for obtaining the use of any telecommunication facility or service, under circumstances that give rise to a reasonable inference that the device has been used or is or was intended to be used to obtain the use of

any telecommunication facility or service without payment of a lawful charge therefore, is guilty of an indictable offence and liable for imprisonment for two years."

Section 327, quoted above, provides for an offence to possess a device to obtain a telecommunication facility or service. In R. v. Duck (1985) 21 CCC (3rd) 529 (Ont DC) the court held that a computer program which functioned to allow the defendant to make long distance telephone calls without incurring any toll charges constituted an instrument or device within the meaning of that Section.

A descrambler used to obtain scrambled pay television signals is covered by this section R. v. Lefave (1984) 15 C.C.C. (3) 287 (Ont. G. Sess. Peace). In R. v. Fuhrer, Alberta Queen's Bench No. 8703 0431C4, November 26, 1987 Justice Sinclair convicted a retailer who sold a decoder to a person enabling that person to receive a scrambled television signal without the requirement of making monthly payments. The sales manager of the company entitled to receive the monthly subscription payment had established to the satisfaction of the Court that the monthly payment was a lawful charge within the meaning of the section. The accused had demonstrated the use of the decoder device to customers going so far as to show a customer a wire which had to be cut inside the decoder so as to unscramble the channel. The accused, however, refused to cut the wire himself. The decoder which was sold and pursuant to which the charge was brought under Section 327 of the Criminal Code had already been altered to allow a customer to pick up the scrambled channel in unscrambled form. The issue in that case was whether the device was of a design which rendered it "primarily useful for obtaining the use of a telecommunication facility or service without payment of a lawful charge". In this case Justice Sinclair convicted after finding the evidence established the charge beyond any reasonable doubt.

As the use of computer systems of computer programs and data becomes increasingly interconnected and therefore increasingly relies on use of various telecommunication systems, the provisions of Section 326 and 327 may become an increasingly important tool in the arsenal of the computer crime investigator or prosecutor.

4.5 Fraud - Sale of Copyright Infringing Goods

Section 380 states:

"(l) Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security,

(a) is guilty of an indictable offence and is liable to a term of imprisonment not exceeding 10 years, where the subject matter of the offence is a testamentary instrument or where the value of the subject matter exceeds $1,000.00; or

(b) Is guilty,

(i) Of an indictable offence and is liable to imprisonment for 2 years, or

(ii) Of an offence punishable on summary conviction,

where the value of the subject matter of the offence does not exceed $1,000.00.

In R. v. Olan, Hudson and Harnett (1978) 41 C.C.C. (2nd) 145, 86 D.L.R. (3d) 212, [1978] 2 S.C.R. 1175, the Supreme Court of Canada considered this provision and held that proof of detriment, prejudice or risk of prejudice to the economic interests of the victims would satisfy the element of deprivation in the offence.

This development was followed by the root case on sale of copyright infringing goods R. v. Kirkwood (1983) 5 C.C.C. (3d) 393, 35 C.R. (3d) 97 (Ontario Court of Appeal). In this case the piracy and sale of video tapes was held to constitute fraud notwithstanding that there was no relationship between the accused and the victim (the holder of the copyright or of distribution rights to the video tapes). This case has been followed in R. v. Fitzpatrick (1984) 11 C.C.C. (3d) 46 (B.C. CA) also involving sale of copyright infringing video tapes.

The theory above which developed, in relation to the sale of copyright infringing video tapes, has also been applied to copyright infringing computer programs and manuals. In R. v. Terrance Ram, Unreported, March 26, 1987 (District Court of the Judicial District of York), the defendant was convicted on three counts of fraud involving unauthorized reproduction of computer programs and manuals. The evidence disclosed at trial showed that the defendant had copied, sold and distributed computer programs and manuals without the consent of the copyright holder. The defendant was convicted on all three counts of fraud and sentenced to five months incarceration on each count, to be served concurrently. In addition, the defendant was placed on probation for three years after release from jail. One term of that probation was that the defendant was not to take part in any business which makes copies of computer programs for rent or sale.

In the Supreme Court of Canada's decision in Stewart, it appears that the Supreme Court may have narrowed the test required in a fraud case from risk of prejudice to economic interests to "real" risk of prejudice to economic interests. In the Stewart case, the confidential information involved was only internally used and the court found that it had no commercial value. As a result, the court found that there was no "real" risk of economic prejudice to the victim and therefore this element of the fraud offence was missing.

The commentary above has shown the use of the general fraud provision in Canada's Criminal Code to deal with a novel argument that being the sale of copyright infringing materials constituting a fraud on the copyright holders. This provision may be of some use in dealing with sale of infringing computer programs, data or other materials. The general fraud provisions, of course, deal more directly with frauds committed through use of the computer as an instrument of crime. This is typically seen in a wide range of cases, such as, for example, cases dealing with abuse of automatic teller machines. Kennison v. Daire (1986) 64 ALR 17 and R. v. Baxter (1987) 11 CRIM LJ 382 (CA).

5 QUASI-CRIMINAL PROVISIONS OF COPYRIGHT LAW

Many forms of abusive behaviour in relation to computer systems, computer programs and data involve the unauthorized reproduction of computer programs or data files. As a result, there are certain remedies which may be available under Copyright law. Generally a civil action for Copyright infringement seeks an interim injunction or Court Order requiring, usually, the Defendant to:

- Refrain from any further unauthorized reproduction of the subject works or any substantially similar variation of those works;
- Seek delivery-up or destruction or disposal of all infringing goods produced; and
- They also seek delivery-up of plates or other items integrally used in carrying out the infringing activity.

It is also possible to seek compensatory damage which would normally only be available only after trial or settlement of the action.

The Copyright Act provides in addition to a broad range of civil remedies for copyright and moral right infringement, a quasi-criminal process under Section 42 for dealing with certain cases of copyright infringement. Section 42 is intended to provide summary remedies and is an attempt to address a fundamental problem in the law of copyright. In modern times and given the spread of reprography, it can be extremely difficult for a copyright holder to pursue civil action against all infringers of his or her copyright. The cost of investigation of the infringement and of the civil prosecution would not, in most cases, warrant the compensatory damages which might be awarded. As a result, Section 42 provides a quasi-criminal remedy under which the State carries out, at the expense of the taxpayer, the investigative and prosecutorial functions.

This section provides:

(1) Every person who knowingly:

> *(a) Makes for sale or hire any infringing copy of a work in which copyright subsists;*
> *(b) sells or lets for hire, or by way of trade exposes or offers for sale or hire any infringing copy of any such work,*
> *(c) distributes infringing copies of any such work either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright;*
> *(d) by way of trade exhibits in public an infringing copy of any such work, or*
> *(e) imports for sale or hire into Canada any infringing copy of such work*

is guilty of an offence and is liable

> *(f) on summary conviction, to a fine not exceeding $25,000.00 or to imprisonment for a term not exceeding 6 months, or to both; or*
> *(g) on conviction on indictment, to a fine not exceeding $1,000,000.00 or imprisonment for a term not exceeding 5 years, or to both.*

(2) Every person who knowingly:

> *(a) makes or possesses any plate for the purpose of making infringing copies of any work in which copyright subsists, or*

(b) for private profit causes any such work to be performed in the public without the consent of the owner of the copyright

is guilty of an offence and is liable

(c) on summary conviction, to a fine not exceeding $25,000.00 or to imprisonment for a term not exceeding 6 months, or to both, or

(d) on conviction on indictment, to a fine not exceeding $1,000,000.00 or to imprisonment for a term not exceeding 5 year, or to both.

In reviewing these provisions note that sale or offer of sale of copyright infringing materials and widespread distribution of infringing materials are the essence of the offence. In this regard it is useful to review some of the copyright implications of use of the internet to identify potential criminal liability.

Most of the material exchanged or released on the internet are works protected by copyright law. As the Internet has evolved from a network providing a means of information exchange to a major new marketplace it becomes more important to review the legal framework for the posting, use and dissemination of materials exchanged on the internet. That legal framework is largely provided by Copyright law.

From a security perspective the rights and remedies provided by Copyright law provide a useful supplement to the physical and administrative security measures. The legal rights and sanctions available under Copyright law also provide a more flexible deterrent and tool than the computer crime provisions of the Criminal Code of Canada.

5.1 What is Copyright?

Copyright law provides a bundle of rights which provide a degree of protection over the form in which concepts or ideas may be expressed. Copyright does not extend to ideas, facts, processes or methods, useful features of works. For example, in the case of computer programs, copyright law protects the form in which the instructions are set out. In the case of a book, copyright protects the phrases used to express the plot but not the concepts underlying that plot. As a result the copyright in an email message, document, musical work or graphic image protects the form of that element but not the ideas contained in it.

5.2 Nature of the Right

Copyright is an intangible right separate and apart from the work which is the subject of copyright protection. It is important to distinguish between the rights of copyright and other rights, such as possession. Possession of a work protected by copyright (ie. this article) may allow the possessor to use the work in many ways but the possessor is not permitted to make copies of the work (or otherwise carry out any of the conduct reserved to the copyright owner). As a result the recipient of an email message or document will generally not have any copyright in the document.

5.3 Types of Works

The type of works available on the Internet appear to fall into the following categories: computer programs, textual materials (ie. notes, messages, documents, poems, plays, dialogue, etc.), graphic images (ie. logos, drawings, etc.), maps, charts, plans, databases, sound recordings, musical recordings, photographs and audio visual works.

Copyright law recognizes virtually all of these as works protectable under copyright. This has significant implications for all users of the Internet and services available on the Internet.

Copyright law recognizes the following categories of works: literary works, musical works, artistic works and dramatic works and also recognizes contrivances used to perform or present certain works (ie. CDs to perform music, etc.). These categories are not rigid and have been expanded by the courts to include new technologies and new forms of expression.

5.4 Scope of Protection

Copyright consists of a number of rights in relation to a work. Subject to the exemptions provided by the Copyright Act or law, that copyright owner is able to either authorize or exclude others from certain activity as follows:

- the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever,

  This right is exercised when the copyright owner posts an email message or document on the internet. The only ability of another person to make copies of or post that message again derive from either permission of the owner or an exemption. Any reproduction of copyright materials (ie. articles, graphic images, etc.) outside the scope of permitted behaviour would be infringing.
- to perform, or in the case of a lecture to deliver, the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof,

  This right is exercised when the copyright owner posts an email message or document on the Internet. Since the Internet site may be accessed by members of the public this is likely to constitute a publication of the work. The only ability of another person to republish that message again derive from either permission of the owner or an exemption. Section 42 of the Copyright Act provides that it is an infringement of copyright to distribute copies of a work to such an extent as to affect prejudicially the owner of the copyright. As a consequence of Section 42 the widespread distribution of a work, without the owner's permission, and even if no payment is sought in respect of those copies may prejudice the rights of the copyright holder and then would be an infringement.
- to produce, reproduce, perform, or publish any translation of the work,

  The only ability of another person to make a translation of a document or message (ie. from English to Greek, etc. and possibly from one computer language to another) derives from either permission of the owner or an exemption.
- in the case of a dramatic work, to convert it into a novel or other nondramatic work,

  This right is exercised when a person converts an email message or document describing the elements of a play into a novel or nondramatic message.
- in the case of a novel or other nondramatic work, or of an artistic work, to convert it into a dramatic work, by way of performance in public or otherwise,

This right is exercised when a person converts an email message, graphic image or document describing a nondramatic document (ie. a story) into a dramatic work (ie. an advertizement, screenplay, etc.).

- in the case of a literary, dramatic or musical work, to make any record, perforated roll, cinematograph film or other contrivance by means of which the work may be mechanically performed or delivered,

  This right is exercised when a person records an email message, image, musical work or document in a form in which it can be played (ie. reproduced). In addition Section 5(4) of the Copyright Act provides certain rights in relation to owners of copyright in digitized musical works released on the internet with the sole right to reproduce it in any material form; publish it, if it is unpublished; and rent it out.
- in the case of any literary, dramatic, musical or artistic work, to reproduce, adapt and publicly present the work by cinematograph,

  This right is exercised when a person adapts or uses an email message, graphic image or document in a film, quicktime movie or the like.
- in the case of any literary, dramatic, musical or artistic work, to communicate the work to the public by telecommunication,

  This right is exercised when a person broadcasts an email message, graphic image or document to the public by some telecommunication means (ie. satellite, broadcast, radio, etc.).
- to present in a public exhibition, for the purpose other than sale or hire, an artistic work created after June 7, 1988, other than a map, chart or plan,

  This display right is exercised when a person displays any graphic image created after June 7, 1988 on any public place other than for purpose of sale or hire. As a result most graphic images displayed on the internet would require the authorization of the copyright owner to be so displayed.
- in the case of a computer program that can be reproduced in the ordinary course of its use, other than by reproduction during its execution in conjunction with a machine, device or computer, to rent out the computer program.

  This right is exercised when a person rents a computer program to others.

5.5 Limits to Copyright Protection

Copyright does not extend to works in the public domain (for example, if the term of copyright has expired). For example, if a person posted the text of Shakespeare's Hamlet the copyright in that play would have expired and it may be used by anyone.

For infringement to take place there must be copyright in the work or there must be no exemption permitting the conduct. In this regard it is important to note that one may copy:

- Works which indicate permission to copy;

  If a document obtained through the internet contains the terms under which the document may be copies or used then the user can rely on the permission provided by the copyright owner. Of course permission provided by someone without the authority of the copyright owner is meaningless and may create the risk of infringement.

  From a security management perspective this illustrates the need to define, implement and enforce standards for access and use of materials provided to or obtained from the internet.

- Where the copyright holder has given permission for the copying;
  In the case of communications or documents made available on the Internet one may reasonably argue that given the nature of the system and the encouragement of copying on the Internet the copyright owner has granted an implied permission to take copies of a work posted on a web site by the copyright owner. Of course if the copyright owner does not wish users to copy the document then the copyright owner can merely state that users are not permitted to make copies. This will defeat any implication of permission to copy.
  Beyond this limited use it is far from clear to what degree other uses of the work may be permitted. For example it is probable that commercial sale of copies of the work is probably outside the scope of any implied permission.
- Works where the term of copyright (for most cases the life of the author plus the end of the year in which the author dies plus 50 years) has expired;
  This will not be an issue for most works presently on the Internet.
- Works created and first published in countries which are not members of copyright treaties with Canada;
  Given the number of countries who are members of the Berne Convention there are few countries to which this would apply. For example, Singapore has no copyright treaty with Canada. As a result a work created and published by a national in Singapore may be unprotected by Canadian Copyright law.
- Under an exemption under the Copyright Act (See below); or
- If a nonsubstantial amount is taken.
  It is not an infringement of copyright to make a copy of a nonsubstantial part of a work.

5.5.1 Exemptions

The most important exemption under the Copyright Act is the fair dealing exemption.

To be exempt activity must be both fair dealing and the within a limited class of permitted exempt activities. The Copyright Act permits copying, without permission of the copyright holder, when such copying constitutes **fair dealing** with the work (ie. no commercial impact on the copyright holder):

> **and** where the copying is carried out for the copyist's own private study or research,
> **or** in the case of fair dealing with a work for the purposes of either criticism, review or newspaper summary if the source and the author's name (if given in the source) are mentioned.

While little case law exists on this point, a rule of thumb to be considered as a guide suggests that generally less than and no more than one copy of a work may be taken for one of such purposes so long as the taking constitutes fair dealing (ie. is equitable). Note that in the Ram, above, case the fact that computer programs were copied for personal profit was sufficient to take the conduct out of this exemption.

Factors which may be taken into consideration in determining if the conduct is fair dealing include:

- The impact of the copying on the copyright owner's economic reward;
- The type of work and its purpose; and

- The amount and extent of the copying.

Other exemptions under copyright law include the "educational" exemption. Section 27 (2) (d), Copyright Act, provides that "short passages", from sources in which no copyright subsists from works not intended for use in schools, suitably acknowledged, do not infringe in school use, so long as "not more than two of such passages from works by the same author are published .... within five years".

Section 27 (2) (f), Copyright Act, provides that recitation in public, of any reasonable extract of a work is not an infringement. See Section 27, Copyright Act, for further exemptions.

It is important to note that the defendant may raise a colour of right defence to such a prosecution. For this provision to be an effective tool the legitimate owner should have in place a policy which sets out, in detail, the basis on which access to the copyright materials is obtained and the basis upon which those materials may be used. These preliminary steps may well serve to result in more successful prosecutions of abusive behaviour.

6 CONCLUSION

It is important that the computer abuse task force respond quickly to gather evidence to provide the basis for successful prosecutions of computer related crimes. The failure to obtain a conviction can have a deleterious affect upon moral and security enforcement efforts. It is therefore important that all reasonable steps be taken, within the limits of the law, to attempt to build the strongest case for successful prosecutions of computer related crimes.

One factor which constantly reoccurs in computer related disputes is the need for competent and knowledgeable expert evidence to assist the court in making its determinations. One should not assume that the courts have any particular facility or understanding of computers, computer programs, or the nature of their operation. As a result, it will be necessary to provide in a simple, accurate and meaningful way, an education for a judge, and jury, if involved, so that the complexities of the technology do not create, by themselves, the uncertainty which leaves a "reasonable doubt" in the minds of the judge and/or jury.

A second important note is that the lawyers prosecuting the action, whether in the area of civil law or criminal law, must very thoroughly brief and understand the complexities of this developing and often uncertain law. In effect, the lawyer will have to educate the judge to understand the nature and scope of the particular law applying to the computer related dispute. In rare cases, a judge may make a decision based on erroneous principles and this can lead to added costs, uncertainty and successful appeals by defendants of convictions. An example of such a case is R. v. Wolfe and Campbell, Unreported, May 16, 1986 (Ont. DC). In that case the defendants were charged with the sale of copyright infringing goods. As discussed previously, there is ample authority to show that the proper offence in such a case is fraud on the copyright holder. Unfortunately, in that case, the judge convicted the defendants but on the basis of theft. The legal foundation for this theft conviction is, at best, tenuous and unreliable. There was no theft of the copyright since you cannot "steal" a right. There is always the danger that errors of this kind create additional uncertainty in the law and may lead to successful appeals of convictions.

A reminder for security professionals involved in cases of computer abuse is the recommendations that:

(a) A computer abuse task force be established and a response plan developed in the event of an incident of appropriate abuse; and
(b) A thorough and comprehensive computer use policy be put into place to provide guidelines for the authorized use of a computer system, computer program or data.

Clarifying the obligations of users of computer systems, computer programs and data serves a legal function but also a more important educational function. Most people are basically honest and once they understand their obligations, will be able to abide by those obligations.

The Sections discussed above are examples of what are anticipated to be the major provisions of the Criminal Code of Canada which would be used in cases of computer abuse. The cases and any further developments both in criminal and civil law should, of course, be noted up and reviewed in detail in any case in which it is anticipated that the applicable Section may be involved. However, these provisions may provide a taste or flavour of the legislation which might apply in this area.

7 BIOGRAPHY

Martin Kratz is an author of various texts and articles including: Control and Security of Computer Information Systems, Computer Science Press (1988) NY; The Computer Virus Crisis (1989) (1992 2nd Ed.), Van Nostrand Reinhold, NY; Information Systems Security: A Practitioner's Guide (1993) Van Nostrand Reinhold, NY; Protection of Copyright and Industrial Design (1995) Carswell, Toronto; Obtaining Patents (1995) Carswell, Toronto. Mr. Kratz teaches Security Law at the University of Alberta and Intellectual Property Law at the University of Calgary. Mr. Kratz is a partner of Bennett Jones Verchere and practices exclusively in the areas of technology law and intellectual property law.