COMPUTER AND INFORMATION ABUSE: NEW LEGAL AND POLICY CHALLENGES +

Donald K. Piragoff*

1989

* A/General Counsel, Criminal Law Policy Section, Department of Justice, Canada. The article represents the views of the writer, and does not necessarily reflect the views of the Department of Justice.

D-1

TABLE OF CONTENTS

D-2

A. INTRODUCTION

Computer-related criminality is one of a number of issues that flow from the rapid increase in the use of computers in the home, school, business and government. Sensational media accounts of various types of abuses, committed either with the use of computer systems or directed at computer systems, have captured the imagination of the public and the legislators. This has been a world-wide phenomenon, and Canada has not been immune from the pressures to legislatively react to perceived or actual problems in the current law. While legislative reaction may be justified in some instances, the issues are complex and the results of ill-considered legislative action may produce unforeseen consequences in other areas of the legal and socio-economic system. Significant study should precede legislative enactment to ensure that the complexities are properly understood and appropriate legislative amendments are made.

The purpose of this article is to identify some of the problems inherent in applying traditional penal laws to the phenomenon of "computer abuse", problems common to both continental European and Anglo-American systems of law; and second, describe Canadian and other countries' responses, and their associated policy justifications and implications.

B. THE NATURE OF THE PROBLEM

"Computer crime" is a term that has come into vogue recently. It is, however, a misleading term. In many instances "computer crime" is legally indistinguishable from existing crimes such as theft, forgery, fraud and mischief (i.e., causing criminal damage). Many abuses involving computers are covered by traditional criminal laws. A bank employee might use a computer to transfer bank funds to a private account and then disappear with the funds. The employee has clearly committed a theft, and has used a computer to assist the commission of the offence. Similarly, a person might use a computer to alter the sum paid to him or her on a paycheque. In each case, the computer has assisted in the commission of the crime. In most countries, the present penal provisions concerning theft and fraud would be adequate to deal with the situations outlined. Consider another example. A person might deliberately damage an automated banking machine outside a bank or might enter an office and steal a computer tape or disk. Again, the present criminal offences of mischief and theft would adequately deal with these abuses. It would be wrong to label these types of conduct as "computer crime". They are really traditional crimes committed with the assistance of computers or with computers as the objects of attack. The traditional laws generally require little amendment to deal with these situations; they appear flexible enough to respond to such abuses.

While many abuses involving computers do fall within the net of existing criminal laws, the development of computer systems, however, has produced a number of legal wrinkles and twists of which earlier lawmakers could not have conceived. There

exist, therefore, certain forms of conduct that, by their nature or by the nature of the entity or phenomenon to which they are directed, are not, or have not until recently been, recognized legally as crimes, although they are clearly considered by many persons to be abuses.

The fundamental question, therefore, is what types of conduct considered to be "computer abuses", should be prohibited by criminal sanctions. Unless it is carefully determined which interests should be legally protected, conduct in relation to computer usage that is perfectly reasonable, merely unethical or simply annoying may be made criminal. Such a course might have disastrous results on the future development of computer technology and have significant socio-economic effects in other areas as well. Legislators and the judiciary must not permit themselves to be awestruck by new technology and over-legislate or over-adjudicate in response, either by creating new offences that unnecessarily duplicate elements of existing ones or by unjustifiably extending the criminal law beyond the types of interests currently protected.

C. A HISTORY OF THE CANADIAN LEGISLATIVE EXPERIENCE

In Canada, legislative response began shortly after the Supreme Court of Canada held that the present offences of theft of telecommunication services or unauthorized use of telecommunication facilities did not include similar conduct committed in relation to computer systems.[1] The Department of Justice of Canada began to develop some legislative amendments, but for various reasons introduction of these proposals into Parliament was delayed. In the interim, two Members of Parliament individually introduced their own Bills (Bills C-628 and C-667) in the House of Commons of Parliament.[2] These Bills, broadly speaking, were aimed at the following: achieving a definition of "computer", an extension of the definitions of "document" and of "telecommunication", the inclusion of computer software and retrievable computer data into the definition of "property" and the inclusion of unauthorized use of programs and data in the laws of theft; penalizing the alteration, damage or destruction of programs and data; and providing for the admissibility of computer records as evidence. Both Bills received only first reading in the House of Commons.[3] It was the opinion of a number of legal and computer experts that the Bills were flawed in both conceptual approach and technical substance, and in some instances, would have over-extended the application of the criminal law. They were, however, useful as educational instruments which highlighted the problem.

Introduced for first reading on December 16, 1982, one of the Bills, Bill C-667, was withdrawn from second reading on February 9, 1983, but its subject matter was referred to the House of Commons Standing Committee on Justice and Legal Affairs.

A Sub-Committee was established which heard evidence from a variety of witnesses. On June 29, 1983, the Standing Committee presented to the House of Commons the Report of the Sub-Committee on Computer Crime.[4] The Report proposed amendments to the Criminal Code[5] and Copyright Act,[6] review of all matters relating to the effective detection and prosecution of computer crime, increased training for police officers and prosecutors, an examination of the feasibility of extending patent and industrial design protection to computer programs, an initiation of a joint federal-provincial study on trade secrecy laws, adoption of appropriate security measures and ethical standards by the computer industry and the introduction of computer ethics in the teaching of computer classes at all levels.

On October 26, 1983, the Government tabled in Parliament a comprehensive response to the Report of the Sub-Committee on Computer Crime that indicated government policy, action and future intensions in the areas addressed by the recommendations.[7] On February 7, 1984, Bill C-19, the proposed Criminal Law Reform Act, 1984, was introduced by the Minister of Justice into the House of Commons.[8] Included were amendments to the Criminal Code to bring the criminal law up to date with respect to the protection of the integrity of computer systems. For various reasons, including a national election, the Bill did not proceed beyond First Reading. On December 19, 1984, the new government introduced Bill C-18, the proposed Criminal Law Amendment Act, 1984.[9] After study by the House of Commons and the Senate, the Bill was passed and received Royal Assent on June 20, 1985 as the Criminal Law Amendment Act, 1985.[10] The purpose of these amendments to the Criminal Code is to ensure that the laws of Canada will protect those who wish to benefit from technology from those who wish to abuse it. The amendments, however, do not address all forms of computer-related criminality in general, but rather are designed to protect the integrity of computer systems.

In the new amendments to the Criminal Code, the Canadian Parliament has charted a cautious course, extending criminal liability commensurate with interests currently protected by the criminal law, while leaving more perplexing questions for further study and analysis. The amendments are really refinements and extensions of six categories of crime that are currently prohibited by the Criminal Code: fraud, theft of telecommunication services, interception of private communications, mischief, misuse of credit cards and forgery.[11]

Specifically, a new subsection has been added to include within the offence of mischief the wilful (a) destruction or alteration of data, (b) rendering of data meaningless, useless or ineffective, (c) obstruction, interruption or interference with the lawful use of data, and(d) obstruction, interruption or interference with any person who is entitled to access thereto.[12] In addition, a new provision provides that

it would be an offence, dishonestly and without a colour of right, (a) to obtain a computer service, (b) to intercept a function of a computer system, or (c) to use a computer system with intent to commit any of the two previously mentioned offences or the offence of mischief when committed in relation to data or a computer system.[13] For the purpose of the existent offences concerning misuse of credit cards, the definition of "credit card" is expanded to include automated teller machine and other types of banking cards.[14] The definition of "document" with respect to the forgery offences is also extended to include, as "documents", computer and other technologically created records.[15]

D. THE DISTINCTION BETWEEN "INFORMATION" AND "DATA"

Although often used interchangeably, there is an important conceptual distinction between "information" and "data". This distinction is important not only for technological reasons, but as will be seen, for legal reasons as well.

Information is not a thing, but a process or relationship that occurs between a person's mind and some sort of stimulus.[16] On the other hand, data is merely a representation of information or of some concept. Information is the interpretation that an observer applies to the data. Different information may be received from the same data depending on how it is interpreted. For example, do the markings on the walls of early cave dwellers represent mere wall decorations or do they represent information or concepts? The meaning is not inherent in the markings. It is only by the interaction of mind and markings that information is caused to be conveyed. For all one knows, Einstein's theory of relatively may be inscribed on the wall of a cave dwelling, undecipherable due to our inability to give meaning to the markings. The same can be said of any language, written or spoken. Particular markings on paper or vocal sounds only have meaning because they represent information or concepts.[17]

In the computer environment, the collection of numerical characters "01100010" has no meaning until some interpretation is applied or an agreement is made to assign a particular meaning to it for a particular purpose. The characters may represent the decimal number 1,100,010, or a binary number whose decimal equivalent may be some other number, or even a word. Different information may be received from the same data depending on how it is interpreted. "Information" and "data" are not synonymous.

Hence, when one destroys or appropriates data, one destroys or appropriates the representation, and not the actual information, idea or knowledge. The latter, for example, may still reside in the mind of the creator, or in the mind of whoever else

may have acquired such knowledge. In order to acquire the information, an acquirer of data must still interpret or decipher the data. It is important to be cognizant of the distinction between "information" and "data" in developing legislation in the area of computer abuse and misappropriation of information.

It is, therefore, significant that the new offences in the Canadian Criminal Code are not in relation to "information", but "data". "Data" is defined in subsection 342.1(2) as "representations of information or concepts" rather than as information per se.[18]

E. THE COMPUTER AS AN INSTRUMENT TO COMMIT TRADITIONAL CRIMES

As indicated earlier, these forms of crime are really traditional crimes committed with the assistance of computers. They include offences such as theft, fraud and conversion (embezzlement) of property (e.g., money or a deposit credit), offences in relation to misuse of credit or bank cards, breach of trust or abuse of confidence, and forgery and related offences. In most cases, penal laws adequately apply. Nevertheless, applicability is particular to a nation's laws: for example, some legal systems do not recognize a deposit credit as property, but only as a claim; some definitions of fraud require that a person actually be deceived as opposed to simply requiring the presence of other fraudulent means or "manoeuvres frauduleuses?" in relation to the use of a machine; and, forgery provisions are sometimes limited by requirements for visual perceptibility or are plagued by other requirements.[19] Since many of these problems are generally country specific, the scope of this article does not permit detailed discussion. Our analysis will turn to abuses causing almost universal difficulty among legal systems.

F. THE COMPUTER AND ITS RELATED ENTITIES AS AN OBJECT OF ABUSE

A typical form of computer abuse where the computer or related entities are the direct target of abuse is computer sabotage, including not only the destruction of hardware and other corporal items such as tapes, disks and micro-chips, but the erasure, destruction or alteration of the data itself. In respect of corporeal items, classic offences such as mischief or causing criminal damage adequately apply. In Canada, for example, the offence of mischief in subsection 430(1) may be committed where a person interferes with what is termed "corporeal" or physical property;[20] for example, destroying paper documents, erasing the ink markings therein or destroying tangible computer tapes and disks constitutes the traditional offence of mischief[21] since a corporeal entity has been damaged or destroyed.

A particular configuration, pattern or arrangement of electromagnetic impulses, however, even if preserved on some physical medium is not corporeal. Thus its destruction or damage, without concurrent destruction of, damage to, or interference with the physical medium, would not constitute the traditional offence of mischief in many countries.[22] Nevertheless, these patterns, configurations or arrangements of electromagnetic impulses can be as valuable as patterns, configurations or arrangements of ink or graphite on a piece of paper. Both forms of configurations, while not information themselves,[23] can represent information or concepts that are susceptible of valuation. Both forms should receive equal protection.

One solution is to amend the definition of "property" in a penal statute to include "data". In Canada, this approach was rejected for a number of reasons. First, section 429, which defines "property" for the purposes of Part XI of the Criminal Code, applies to more offences than simply mischief. For example, it is difficult to conceive of the burning of electromagnetic impulses in such a way that the arson provisions could apply.[24] Second, some of the types of conduct that constitute mischief in relation to corporeal property can have no application to incorporeal computer data.[25] Third, there exists a distinction between information and data as discussed earlier. Fourth, the inclusion in the definition of "property" of any reference to "data", which has been defined to include "information", creates the dangerous inference that information per se may be considered to be property.[26]

Accordingly, the best solution was to create a new provision concerning mischief in relation to data that parallels the offence of mischief in relation to corporeal property.[27]

In Canada, the ordinary offence of mischief in relation to corporeal property not only includes the destruction or damage of property, but also the obstruction, interruption or interference with the lawful use, enjoyment or operation of corporeal property or with any person in the lawful use, enjoyment or operation of such property.[28] If wilful acts deny a person the lawful use of computer equipment, they would constitute the offence of mischief, since the object interfered with is corporeal. For example, wilfully interfering with the power supply to, or overloading the input capacity of a computer system could constitute mischief.[29]

Similarly, in many countries, while the actual destruction of data in incorporeal form does not constitute mischief, the consequential effects upon corporeal property may nevertheless constitute the offence of mischief.[30] This is based on the rationale that the destruction of computer data, for example, has damaged or interfered with the functional integrity or use of the corporeal computer tape or disk. In the Canadian case of Regina v. Turner,[31] the accused altered intangible computer programs that

were contained on computer tapes, with the result that the programs would not operate properly. While the alteration or destruction of the incorporeal data did not constitute the offence of mischief, the resulting interference with the use of the corporeal tape containing the altered incorporeal data was held to constitute mischief.

Yet, despite the applicability of provisions such as those above, they are nevertheless still deficient. First, they do not directly attach penal liability for the interference with the data, but rather attach it to the consequential effects upon corporeal property. If the interference is only in relation to the use of electromagnetic impulses, for example, with no corresponding interference with the use of corporeal equipment, no offence of mischief occurs. It is preferable that the interests directly protected by society in offences concerning mischief in relation to corporeal property be equally protected where the asset is incorporeal, such as in the form of computer data. In Canada the legislative solution was to create a specific offence of mischief in relation to data where a person wilfully and without colour of right, lawful excuse or justification, destroys or alters data, renders it meaningless, useless or ineffective, interferes with its lawful use, interferes with any person who is lawfully using it or denies access to any person entitled thereto.[32]

While statutes concerning mischief in relation to corporeal property usually contemplate only destruction or damage as constituting a delict deserving of punishment, the alteration of data (e.g. by inserting new data into a computer file or program, even without any destruction of existing data) is equally destructive of the integrity of the original data, and equally deserving of legal sanction. Accordingly, the new law in Canada not only includes within its scope unauthorized destruction of data, but also unauthorized alteration of data.[33]

Offences of mischief or causing criminal damage to property or data are not only important because they reinforce and protect societal interests in the preservation and maintenance of the integrity of property or data, but interference with integrity can have disastrous consequences to human life; e.g. interference with the integrity or use of medical or air traffic control computers or data. While such acts may in some cases be addressable directly under penal provisions concerned with endangerment to life, one should ensure the equal application of any particular offences that concern interference with property that causes endangerment of life. In Canada, subsection 430(2) provides that mischief that causes actual danger to life is a separate and more serious crime. The classification of the new data offences in section 430(1.1) as "mischief"[34] ensures equal applicability of subsection 430(2) to both property and data interference.

It is also important to note that data does not have to be within a computer at the time of its destruction, alteration or interference. Computer data may be attacked in the course of telecommunication or by placing a strong magnet, for example, in close proximity to a tape or disk, thereby erasing or rearranging the electromagnetic representations recorded therein. In Canada, the use of the phrase "in a form suitable for use in a computer system" in the definition of "data",[35] as opposed to "in a computer system", includes within the scope of protection not only data in transmission but data in computer media which may not, at the relevant time, be in direct association with the computer system. With the refinement of optical readers and audio input and output, this definition could in future include program source code or other data in hard copy form, such as writings on paper, and oral speech.

Of course, merely causing damage or interference is not enough to justify criminal liability. A culpable state of mind must also exist. In Canada, safeguards designed to exclude the accidental or otherwise lawful alteration, destruction or interference with use of data and the intentional alteration or destruction of one's own data have been included in the definition of the offence. The requisite mens rea or mental element would require that the conduct be performed "wilfully";[36] that is, either (i) knowingly and intentionally, or (ii) with the knowledge that the conduct will probably cause the event to occur and with subjective recklessness as to whether the event occurs.[37] Furthermore, subsection 429(2) provides that no person can be convicted of mischief if he or she "acted with legal justification... excuse or...colour of right". A colour of right would include any situation where the person, although mistakenly, honestly believed that he or she had a right to destroy, alter or interfere with the data.

G. ABUSIVE CONDUCT IN RELATION TO COMPUTERS OR DATA

The previous section generally discussed situations where the computer or data were the direct objects of abuse. This section discusses various abuses in relation to the use or misuse of computers or data.

1. Interference with Lawful Use

This includes all types of unauthorized obstructions, interruptions or interferences with the use of computer systems or data. Although conceptually belonging under this classification, these abuses were discussed under the previous part both for analytical purposes, and due to their relationship to mischief or criminal damage offences.

2. Interception of Communications or Functions of a Computer System

Even if there is no alteration or destruction of, or interference with the use of data, the intrusion into the computer system, interception of communications or gaining knowledge of other inner-workings or functions of a computer system represents a serious violation of privacy.

In other areas of the law, countries have sought to protect the integrity of particular communication systems or types of communications. This protection has often been afforded independently of the nature, status, secrecy or content of the message being communicated. This type of protection finds its form in laws concerning wiretapping of communication systems or other more general types of electronic surveillance of communications, whether in electronic or oral form. The statutes of many western legal systems, however, only apply to the interception of oral communications or conversations between persons,[38] and have limited or no application to the interception of communications of computer systems, let alone to the interception of any other valuable function that may be performed.

Likewise in Canada, the ordinary laws prohibiting theft of telecommunication services[39] or interception of private communications[40] would not, cover many instances of accessing or otherwise gaining knowledge of the communication of data or other internal processes (i.e, functions) of a computer system. The ordinary wiretap or electronic surveillance offence[41] arguably applies where two persons,[42] by means of telecommunication,[43] link their computers together and communicate with one another. This law would probably not apply, however, to the following situations: communication between two computer systems belonging to the same person; two computers communicating with one another rather than with the persons who own them; one computer system communicating with itself; or communication between a computer and a person.[44]

With the increasing inter-relations, and difficulty in distinguishing, between telecommunication systems and computer systems, it is important that the law adequately protect both computer systems and their communications from unauthorized surveillance. It is important to note that the interests to be protected include not only the transmission of data communications within a computer system, between computer systems and between computer systems and persons, but also the surveillance of other internal or external processes or functions of a computer system. In the course of their operation, computer systems perform many other functions besides data communication. In addition

to data processing, these include inter alia logic, control, arithmetic, deletion, storage and retrieval. Surveillance of a computer system can reveal the inner or external processes or functions of a system. These functions can be just as valuable, and their surveillance can be as much a violation of privacy, as the interception of telecommunication or communications of data.

In Canada, paragraph 342.1(1)(b)[45] of the new law has, therefore, been enacted to address not only the uncertainties of the former law with respect to interception of telecommunications or communications, but also the new privacy interests created by the computer age. It provides that "every one who, fraudulently and without colour of right...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..."is guilty of an indictable offence or an offence punishable on summary conviction." For the purposes of this provision "intercept" includes "listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof." The term "function" is defined to include "logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system".[46]

Generally, one can only "intercept" a function of a computer system if there is some aspect of communication, either internal or external, engaged in by that system.[47] This interception can occur either directly, through the access and use of the computer system (by using one of its terminals, for example), or indirectly, through the use of electronic eavesdropping devices. These latter techniques do not have to involve any direct access to or link with the computer system, and can include inductive coupling, the reception of advertent electromagnetic broadcasting or the reception of inadvertent electromagnetic broadcasting of radiation from various components of a computer system. For this reason it is important that legislative solutions not be limited merely to proscribing unauthorized "access" to a computer system or to computer data.[48] More is at stake than simply data; and surveillance and interception techniques go beyond unauthorized access or entry to the physical computer system.

Accordingly, by use of the concept "intercept" the new Canadian law addresses conduct of a scope that is broader than mere "access" to the computer system. Also it is the surveillance or interception of a "function" of that system, rather than the interception of the "data" itself that is prohibited by paragraph 342.1(1)(b).

It is, of course, true that this new provision would indirectly prohibit the unauthorized acquisition of data from a computer system. If the interception of a function is prohibited, this will necessarily prohibit the unauthorized acquisition of the data that may be contained in that function.[49] This provision, however, does not seem to be aimed directly at the issue of appropriation, but rather at interception and the violation of privacy interests. Like the current wiretap offence in the Criminal Code,[50] the gravamen of the new offence is not an acquisition or appropriation in the manner or nature of theft,[51] but rather the unauthorized surveillance and gaining knowledge of a communication or other processes to which one is not entitled. For example, when one's telephone conversation is intercepted, no one conceptualizes the wrong as a theft of the communication or the information. In many instances, the communication may be of no real extrinsic value; e.g. a marital conversation between spouses. The gist of the delict is the violation of privacy, independent of the nature of the communication. Therefore, just as the law grants a right to privacy and protects the integrity of personal communication with another person, the new provision grants a similar right in respect of the integrity of one's computer system. In other words, one has the right to communicate with one's computer system in private as well as the right to have the computer communicate externally to oneself, internally with itself, or privately with other computer systems.

The issue of unauthorized acquisition of data or information as a delict deserving of punishment will be discussed later. It will be found that unlike the case of privacy interests, the context of the data or information acquired may be crucial to determining whether and in what manner any crime of misappropriation should be defined.

Being criminal conduct, statutes prohibiting access to or interception of computer functions require techniques to distinguish criminal wrongs from civil wrongs. Existent and proposed restraints on over-criminalization vary among countries. Some countries have established or proposed objective requirements, such as the necessity that security measures be infringed before liability attaches.[52] Other countries,[53] including Canada, have limited criminalization by requiring that the accused possess particular culpable states of mind, independent of whether the target of the attack was properly safeguarded. In Canada, for example, it is necessary that the interception be performed "fraudulently and without colour of right".[54] The term "fraudulently" in Canadian law essentially means dishonestly; the commission of a fraud is not necessary. To act without a "colour of right" is to act without any honest belief that one had a right to perform that act. The necessity to break any security systems,

or the lack of any security, however, could affect the state of that belief. In effect, objective criteria, such as the degree of security, is subsumed within the subjective mental element.[55]

3. Unauthorized Use of Computer Systems

Although inter-related, for analytical purposes this topic will be discussed under two separate heads: a) the unauthorized obtaining of computer services or time, and b) the unauthorized use of computer systems in general. The delict in respect of the former is the unauthorized obtaining of data processing or other services, while the delict in respect of the latter is the unauthorized use of the computer itself. Some countries' laws, or proposals for reform, cover only one delict, some cover both and some have separate offences for each.

a) Unauthorized obtaining of computer services or time

In some countries, the classic offences analogous to obtaining computer services are those concerning the unauthorized use of automatic vending machines or public telephone networks, and general theft of service laws. While general theft of service[56] laws may apply in such cases, the application of other provisions directed at the use of vending machines or telecommunication facilities is less certain. Some laws are restricted to services offered for a fee.[57] In other laws, computer systems have been held not to be included within the purview of statutes prohibiting theft of telecommunication services or use of telecommunication facilities, such as in Canada.[58] In some countries, statutes concerning the unlawful use, waste or withdrawal of electricity are applicable;[59] while in other countries they are not.[60]

In some countries, such as Canada, other offences of general application have been held to apply in some circumstances. For example, where an account number has been assigned to a lawful user and a person falsely represents himself as having authority to debit the account and use computer time, the person may be prosecuted for fraud under section 380 of the Criminal Code. Prosecutions in respect of the offence of fraud have been successfully undertaken based on the monetary worth of the service debited to the lawful user's account.[61] Where a person falsely assumes the identity of a lawful user, a charge of personation under section 403 of the Criminal Code may be applicable.[62] In some countries, such as the United States, general theft provisions have in some instances been held to be applicable to the "theft" of computer time, due to the particular nature of the wording of the provisions.[63]

Since computer time or services has economic value, it is logical that its misappropriation should be sanctioned as equally as are the misappropriation of other things of value of which a person can be deprived. In the United States of America, many States have enacted specific theft of computer service laws, amended definitions of "property" or included such conduct within special omnibus provisions on computer crime.[64] In Canada, a specific prohibition was created in respect of the obtaining of "computer services" if the services are acquired dishonestly and without a colour of right.[65] Other countries also have proposed specific provisions.[66]

b) Unauthorized Use of Computer Systems

The obtaining of computer services or time (discussed above) is, of course, one aspect of the broader concept of unauthorized use of computer systems. In fact, the unauthorized use of a computer system is inherent in the commission of most computer abuses and traditional crimes where the computer is used as a means, although there are some situations where the direct use of a computer is not required; such as where a tape is erased by placing it in close proximity to a strong magnet, or a function of a computer system is intercepted by the use of electronic eavesdropping devices.

The concept for present discussion, however, is whether and to what extent should the law penalize the mere unauthorized use of a computer system. Unlike the obtaining of computer services or time, the type of use under present discussion may result in no deprivation of use or of monetary value to the owner (other than electricity consumption costs). Essentially, the proffered interest to be protected is the value of exclusive use of a computer system for its owner.

In many countries, criminalizing such conduct poses little difficulty. Some countries possess laws of general applicability against the unauthorized or illegal use of another person's property.[67] In other countries, however, the law, only penalizes the use of specific types of property, such as automobiles,[68] or only penalizes use where the victim has suffered a loss or inconvenience.[69] In some countries the general offences of theft or conversion may be applicable where the use of property amounts to a conversion. Yet, in many situations of unauthorized computer use, the requisite intention to deprive the owner of property (the computer) or of its exclusive use may not exist.

One advantage of criminalizing unauthorized use is that it attaches liability at a stage prior to the actual causation of more serious types of harm. Given

the highly sensitive and critical uses to which computer systems can be employed, the potential for the manifestation of actual harm is great. In fact, in some respects the type of interests affected are similar to those inherent in penal laws against trespass to real property. The delict could be characterized as "computer trespass". Along with interception or surveillance of computer systems, this type of conduct may be the goal or limit of many so-called "computer hackers" who are only interested in boosting their egos by meeting the challenge of obtaining access to a system and taking an electronic ambulation within its circuits.

If a nation chooses to penalize such conduct, various legal techniques exist. One technique is the creation of general offences concerning unauthorized use of property.[70] This, however, may not be a socially acceptable technique for some countries. Alternatives include the extension of offences concerning unauthorized use of telecommunication systems or the creation of specific offences concerning unauthorized use of computer systems. The latter approach has been adopted in Canada and, either proposed or adopted, at both the federal and state levels in the United States of America.[71] Many of these proposals or statutes use the term "access", but the definitions of that term which are employed in these proposals or statutes are not restricted to entry, but essentially mean "use".

In designing sanctions for the unauthorized use of a computer system, a major concern must be whether a society wishes to criminalize the mere authorized use of a computer, especially since a computer can conceptually include not only a large mainframe, but also certain wrist watches or microwave ovens. The inclusion of a new offence of "unauthorized use" would require safeguards to ensure that criminal sanctions only attach to those situations that are regarded by society as involving moral turpitude. Moreover, criminal liability should not attach to persons who, acting innocently, honestly believe that they have authority to use a computer.

This concern to limit the scope of liability is reflected in the various definitions of "computer" that exist in the statutes of a number of jurisdictions. Many of these jurisdictions exclude such devices as pocket calculators,[72] "automated typewriters or typesetters" and "routine personal, family or household" computers.[73] Nevertheless, these definitions of "computer" are still broad enough to include certain wrist watches and even microwave ovens. Furthermore, there is no functional difference between small business computers, personal use computers and large mainframe computers.

A dilemma, therefore, arises in attempting to legislate in this area. If the legislation is too specific it may be technologically or functionally limited in the types of computers it protects. If the legislation is too general, it may penalize any unauthorized use of a computer system, or punish persons who honestly thought they had authority to use that system. For example, does a society really wish to punish criminally a person who, with knowledge of his lack of authority, enters a colleague's office and uses that colleague's desk-top calculator or mini-computer? Surely, not. However, if the person's use is not simply for his own purpose, but is intended to destroy data, survey data or change a calculation in a manner that could cause financial harm, the application of the criminal law would probably be viewed as acceptable by society.

In Canada, Parliament resolved the dilemma by inserting limits and safeguards into the mens rea or mental element that is necessary to constitute the offence, rather than into the definition of "computer system". While the definition of "computer system" and the physical element of the offence are broad in scope, the mental element is narrow. The mens rea has been defined so as to include the concepts of "fraudulently", (that is, dishonestly) and lack of "colour of right".[74] The concept of dishonestly imports that element of moral turpitude that gives crimes their special character, distinct from other unauthorized conduct. The addition of the concept "without a colour of right" addresses the situation of the person who honestly, but erroneously, believes that he has the authority to use the computer system in the manner in which he actually used it.

Unlike the new offences of obtaining computer services or interception of a computer function, additional safeguards have also been included in the new offence of unauthorized use. In addition to the above requirements that the conduct be dishonest and lack a colour of right, there is a further requirement that the computer system be used with the intent to cause other types of computer abuses or harm.[75] These include destruction of a computer system, destruction or alteration of data, interference with the lawful use of a computer system or data, or unauthorized obtaining of computer services or interception of a function of a computer system. It would not be an offence to gain access to or otherwise use a computer system without the further intent to cause the types of harm specified.[76]

The mental elements vary among the three offences, because different interests are being protected. The first offence, obtaining "computer services", protects the same interests inherent in offences concerning theft of services; the second

offence, interception of a function of a computer system, protects privacy interests; and, the third offence protects the right of exclusive use of one's property, and penalizes trespass with intent to misuse the property. Different policy considerations apply to various types of delicts, necessitating appropriate mental states of culpability. Somewhat similar approaches can also be found in various American statutes, and in the proposals of the Scottish Law Commission.[77]

Since, the new paragraph 342.1(1)(c) requires that there need only be an intent to cause harm or other abuses through the use of a computer system, the offence has the added benefit of not requiring the proof of actual harm, which some of the other offences require. This may also have the advantage of permitting a prosecution without requiring the complainant to publicly divulge the details of what was altered, destroyed or intercepted, an important consideration if the data is of a confidential nature. The mens rea requirement that there exist a lack of colour of right on the part of the perpetrator may have the added societal benefit of prompting employers, universities or other owners of computer systems to set ethical guidelines for users with respect to what is proper and improper conduct in respect of computer systems. An honest, even though erroneous, belief in a right to use the computer system will always negative culpability.

H. UNAUTHORIZED ACQUISITION, DISCLOSURE OR USE OF INFORMATION AND DATA

The increasingly technological nature of society, the growth of new information industries, and the need to remain competitive in the market place have made misappropriation of information an attractive commercial alternative to the outlay of expensive research and development costs to generate that information within one's own business. Solutions to the problem however, are not easy, and solutions that are too restrictive can have counterproductive effects.

Earlier, we discussed the distinction between "information" and "data". Data is a representation, in either tangible or intangible form of information or of some concept. Information, on the other hand, is not a thing, but a process or relationship that occurs between a person's mind and some sort of stimulus. It is the interpretation that an observer applies to the data. Even if there is only one representation or set of representations (i.e. data), the interpretation (i.e., information) can be acquired, shared or possessed by more than one person. These basic distinctions between the two concepts have profound implications on the

manner in which the law treats the unauthorized acquisition, disclosure or use of data or information.

Unauthorized copying or other uses of data are usually conceptualized as violations of copyright law since copyright protects the form of expression, rather than the content.[78] Many countries are reviewing their copyright laws to ensure that representations of concepts or information (i.e., data) in the form of computer programs or micro-chips are adequately protected.

If a particular set of data is in a tangible form, dishonest asportation and fraudulent dispossession may be remedied by traditional laws of theft, fraud and other-property related penal laws. If the data is in intangible form, problems may arise in the application of these laws. For example, can oral representations, such as human speech, be stolen? What about electromagnetic impulses?

For the purpose of discussion, however, we will concentrate on "information", rather than "data". Being a process or interpretation, information is always in intangible form, as opposed to the data which represents it or the medium upon which the data may be recorded. Thus, difficulties in the application of traditional law are manifest. Furthermore, the unauthorized acquirer, discloser or user is interested primarily in the information content, and not necessarily in the representation.[79]

Traditionally in western legal systems, information, as distinct from the medium upon which it may be recorded, could not be the subject of classical theft.[80] Traditional theft statutes cause problems generally in three areas. First, they usually require that the subject matter be taken or subject to some other form of asportation or dispossession. While one can "take" a disk, tape or print-out since these are tangible, there are some things of which it is difficult to conceive as being "taken". Just as one can take, and thereby steal, a ticket to a theatrical performance, one can take a magnetic tape, disk or sheet of computer print-out paper containing representations of information. The viewing of the theatrical performance, however, has not been "taken", and it can be argued that neither has the information. "Taken" is not synonymous with "acquired" or "obtained". Merely because a person acquires information, does not mean that that person has taken it. The point is clearer if we consider the situation of a person who, on a remote terminal, obtains or has flashed on his or her video screen a copy of someone else's data file. The victim still retains the data file unaltered and still possesses its informational content. Nothing has been taken; only the data copied (and possibly the informational content acquired if the data was not encrypted).

Second, these offences usually require either an actual deprivation of or an intention to deprive the victim (usually permanently, but sometimes even temporarily) of that which was taken or converted. In the above example concerning copying, it can be argued that there has been no intention to deprive. The victim retains the data file and the information; and there may have never existed any intention to deny such retention, but only to become appraised of the contents and nature of the data file.

Third, these offences usually require that the subject matter be corporeal or, if incorporeal such as a deposit credit at a bank, that it be capable of constituting "property". The incorporeal nature of computer data and information per se, render difficulties, however. The ascription of full "property" status to information raises not only conceptual, but socio-economic problems, as will be discussed later.

Nevertheless, despite these difficulties courts in many countries have been twisting traditional laws to apply. In France,[81] the Netherlands[82] and the United States of America,[83] courts have applied theft statutes to the photocopying of a document or copying of computer data and programs. In these cases, courts have usually been influenced by the fact that for some brief period of time the original documents or programs were in the hands of the perpetrator before the copying. On the other hand, one American state court had doubted the applicability of such laws, if the information was only memorized without any asportation of the media.[84] Other American courts had also refused to make such extensions of the law.[85] In the past, the situation in the United States often appeared to depend on whether a classical theft statute was being considered or instead a differently worded statute concerning specific prohibited conduct in relation to property, such as inter-state transport or obtaining of stolen goods or property.

In 1987, however, the United States Supreme Court, in the case of Carpenter v. U.S., considered a federal statute that prohibited "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretences". In this case, the accused agreed with others to provide the latter with advance information as to the timing and contents of a column which appeared regularly in the Wall Street Journal. The column concerned the Stock Market, and due to its prestige could affect the price of stocks on the exchanges. White, J., for the Supreme Court, held that the Journal had an "interest in the confidentiality of the contents and timing of the column as a property right" and that they had "a property right in keeping confidential and making exclusive use, prior to publication, of the schedule and contents of the column."[86]

In the United Kingdom, the Court of Criminal Appeal refused to extend the concept of property to confidential information in a case involving the misappropriation (alleged theft) of the contents of a university examination paper.[87]

In Canada, the Ontario Court of Appeal, in Regina v. Stewart[88] [by a split decision (2:1)] in reversing the decision of the trial judge, held confidential business information to be "property", and found the accused guilty of counselling another to commit theft, and fraud, when he attempted to persuade the other person to surreptitiously obtain a list of employees from the files of a hotel during the course of an industrial dispute.

On further appeal, the Supreme Court of Canada, however, in a unanimous decision, held that whatever the legal classification might be for the purposes of the civil law, information was not property for the purposes of the criminal law.[89] Lamer J. for the Court, reviewed various public policy considerations involved in ascribing a property status to confidential information[90] and held, that as a matter of policy, confidential information should not be property for the purposes of the theft provisions of the Criminal Code. "[T]he realm of information must be approached in a comprehensive way, taking into account the competing interests in the free flow of information and in one's right to confidentiality, or, again, one's economic interests in certain kinds of information. The choices to be made rest upon political judgments that, in my view, are matters of legislative action and not of judicial decision."[91]

Even assuming that information could be considered as property for the purposes of the criminal law, the Court also concluded that the concept of theft, as proscribed in the Criminal Code, would not apply to the misappropriation of information. The Court referred to the problems associated with the requirements for asportation and deprivation of the thing taken or converted (as discussed earlier), as being reasons for denying the applicability of section 283 [now s. 322] of the Criminal Code.

Throughout the various levels of the judicial history of the Stewart case, the various court decisions have been both applauded and criticized by other courts and academic commentators.[92] The scope of this article does not permit an in-depth analysis of this issue, except to say that, in the opinion of the present writer, the discussion concerning the concept of "conversion" can be severely criticized, but that essentially the result of the decision with respect to the property issue is correct; that is, information per se cannot be considered to be property. The Court, however, could have undertaken a more in-depth analysis of the issue, and failed to draw a distinction between holding that information per se (and even confidential information) could not be "property", and recognizing that in some circumstances

(e.g., a trade secret) one may have a proprietary right in the information, which could be adversely affected by an unauthorized acquisition, disclosure or use of the information.[93] Depending on the elements and structure of the offence under consideration, this property right could be the subject of a criminal offence. In this regard, it should be recalled that the United States Supreme Court in Carpenter v. U.S. (discussed earlier), tended to frame their analysis in terms of a property right or interest in the information (i.e., right to confidentiality and exclusive use) rather than that information per se was property.

Even in Stewart, the Supreme Court recognized that the offence of fraud could have been committed if, by the unauthorized acquisition, the hotel had suffered a financial or commercial detriment or deprivation. In addition to "property", one can also be defrauded of "money" or a "valuable security" under section 380. However, there was no intention on the part of the hotel to deal in a commercial way with the confidential information, and it was "difficult to see how the hotel had suffered the requisite deprivation or detriment within the meaning of R. v. Olson, supra. The deprivation would be clear if the confidential information had been in the nature of a trade secret or copyrighted material having a commercial value intended to be exploited by the victim."[94] Therefore, depending on the circumstances, the offence of fraud may be available with respect to some misappropriations of information.

In some American states,[95] legislators have specifically defined computer data, information or trade secrets as "property" or a "thing of value" subject to theft. For purposes of consistency in policy, however, misappropriation of information from a computer system should not be a criminal offence if the same conduct in a non-computer environment is not criminally culpable. In Canada, the Parliamentary Sub-Committee on Computer Crime specifically rejected any course of action that would "confer on computer-stored information a status different to that of conventionally stored information".[96]

Although discussed to some degree to by the Supreme Court of Canada in Stewart, many of the judicial and legislative attempts to tackle misappropriation of information through extension of property concepts have failed to recognize the broader issues involved. A determination of whether information should be given proprietary status for the purposes of the criminal law, or whether a particular statute can be read as applying to the misappropriation of information cannot be decided purely within an analysis of criminal law principles or statutory interpretation. Other areas of law, such as intellectual property law, must be considered as well as broader policy issues.

The issue of the unauthorized acquisition, disclosure or use of information raises a number of legal, social and economic issues. The shift to a post-industrial society

raises two critical challenges to society in respect of information. The first relates to the ability to devise new legal, economic and social arrangements and protections that will ensure both the creation and the effective and profitable utilization of new information and technology. The second, challenges a liberal society to protect its basic political, economic and human values from unwise applications or withdrawals and restrictions of that new knowledge. On one hand, the law must provide creators or holders of information with legal protection. Creators may be reluctant to invest time and money in research and development if the results of their efforts can be freely appropriated by others. On the other hand, one does not wish to unduly restrict the free flow of information, such that information or knowledge monopolies may be created as a result of the law conferring exclusivity. A free flow of information generally benefits society. Research and information generation can be expensive, duplication of effort is wasteful and a legal regime which creates excessive restrictions on the free flow of information promotes further espionage.

To a large extent, the advocates of the "information is property" debate have raised the first societal challenge as justification that not only should information be legally protected, but that it should be given property status. Lately, however, a number of writers have begun to focus on the second challenge and have examined how excessive secrecy or protection, and laws that permit such, are arguably leading to a retarding of innovation, limiting of competition, monopolization of technological and research initiatives and the use of these protective laws as a commercial weapon rather than as a protective shield as originally conceived.[97]

Any legal solution must be flexible enough to balance these two conflicting interests. Various laws in western society, both common law and statutory, exist in respect of the legal protection of information; for example, laws in respect of state secrets, trade secrets, copyright, patent, trademark, contracts, employment law, fiduciary duties, economic torts, privacy, access to information and breach of confidence. These laws have generally recognized the need for a balance. For example, copyright and patent laws can, if certain conditions are met, grant exclusive rights for limited periods of time to an individual to use particular types or forms of representations of information, knowledge or ideas; but even these laws do not transform that which is patented or copyrighted into a form of traditional property. Privacy, personal data protection and access to information laws provide other good examples of where legislators have realized the necessity for legal vehicles to possess flexibility in order to resolve competing policy interests.

In the 19th Century, property was ideally defined as an absolute dominion and exclusivity over things. Such a concept is no longer credible. Property is now more properly understood in terms of equities and relations. Property rights are the

societally sanctioned behaviour relations among persons that arise from the existence of goods and pertain to their use.[98] However, different types of information have different types of relational equities among persons and between the state and the individual. For example, the public policy considerations differ amongst personal information, information held in government hands, public information, research and academic information, and commercial or business information. Different factors have to be considered and different balances struck when affording legal "rights" of protection. These examples point out that the assertion of rights, including property rights, is a conclusory statement; it derives from a consideration of and balance of the issues, and reflects a conclusion to protect a particular interest. To suggest as the starting point of the analysis that information is "property" ignores the balancing of the issues required and avoids the critical questions: (i) Why should this information be protected? and (ii) If the information should be protected, to what extent and in what manner?

Many different kinds of information exist, and they will be appropriated under differing circumstances. Any legal regime should aim at providing a range of remedies, both civil and criminal, for such misappropriation, as well as maintaining a proper balance between information flow and protection. No single reform measure will suffice, nor can all types of information be treated in the same manner. Different policy considerations arise concerning acquisition, disclosure or use depending on whether the information is commercial in nature, personal, governmental, etc. The law, in both its civil and criminal aspects, should provide a range of remedies. The civil and criminal law dimensions of "information protection" are clearly linked, and may conceivably serve a common set of policy goals.

In Canada, the Parliamentary Sub-Committee on Computer Crime, also studied a number of issues involved in the protection of information. The Sub-Committee stated that Parliament would be ill-advised to try to protect information by granting a proprietary interest in it.[99] Recognizing the dual criminal (federal) and civil (provincial) aspects, the Sub-Committee recommended instead that a joint federal-provincial study be undertaken concerning trade secrecy laws with a view to developing legislation to address the misappropriation of information. A federal-provincial study was initiated and its final report was completed in 1986.[100]

The report of the federal-provincial study examines the current state of legal protection of trade secrets, the policy justifications for civil and criminal law protection and proposes the enactment of new civil and criminal legislation to address the unauthorized acquisition, disclosure and use of trade secrets and confidential business information. Rather than adopting an approach based on property or fiduciary relationship, the report bases its recommendations on an

entitlement approach to information; that is, it is necessary to determine first the reasons why a particular type of information should be protected and why persons should or should not have access and, second, if there should be an entitlement to protection, under what circumstances and limitations. The report proposes two schemes for civil and criminal law protection that attempt to take into account the need for adequate limitations and safeguards.

A review of trade secrecy laws, including commercial secrets, is also occurring in a number of European countries as well.[101] A major review was completed in the United States in the late 1970's.[102]

Once legislators have balanced the competing interests inherent in this field, it is recommended that their attention turn to other types of information so that eventually a sound and consistent information policy can be achieved. Legislators in enacting new computer-related or information crime laws, and courts in interpreting both traditional and new penal laws, must be careful not to create counter-productive effects in other areas, by over-extending either the reach of the criminal law or concepts such as "property" which may be ill-suited to the vagrancies and competing policy interests of differing kinds of information.

Pending the completion of these various "information" laws that would directly regulate the unauthorized acquisition, disclosure or use of various types of information, preferable solutions in the computer area have been to address liability to the unauthorized access to or use of computer systems, or to the unauthorized surveillance and interception of their functions, as discussed earlier.[103] Similar approaches have been recommended by the Organization for Economic Cooperation and Development and the Council of Europe.[104]

I. CONCLUSION

As indicated in this article, while legislative or judicial action may be justifiable in some instances, the issues are complex and the results of ill-conceived legislative or judicial action may produce unforeseen consequences in other areas of the legal and socio-economic system. Significant study should precede legislative enactment or judicial action in order to ensure that the complexities are properly understood. One must be careful in determining which interests should be legally protected, otherwise conduct in relation to computer or information usage that is perfectly reasonable, merely unethical or simply annoying may be made criminal. On the other hand, a failure to appreciate the subtleties of the new technology or new economic or information relations may result in clearly blameworthy conduct escaping the net of criminal liability. Computer and information abuse pose, and will continue to pose, new legal and policy challenges in the coming years.

ENDNOTES

+ Portions of this article have previously been published under the title "Combatting Computer Crime with Criminal Laws", in Computermisdaad en Strafrecht, (ed.), H.W.K. Kaspersen, Kluwer rechtswetenschappen, Antwerpen, Belgie (1986), at 103

1. R. v. Mclaughlin, [1980] 2 S.C.R. 331.

2. Bill C-628, An Act to amend the Criminal Code (computer crime), 1st Session, 32nd Parliament, 29-30 Elizabeth II, 1980-81; Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, 1st Session, 32nd Parliament, 29-30-31 Elizabeth II, 1980-81-82.

3. Bill C-628 died on the Order Paper when the First Session of the Thirty-second Parliament ended in December 1983. Bill C-667 was withdrawn from second reading on February 9, 1983, and its subject matter referred to the Standing Committee on Justice and Legal Affairs.

4. Report of the Sub-Committee on Computer Crime, being the Ninth Report of the Standing Committee on Justice and Legal Affairs, 1st Session, 32nd Parliament, 1980-81-82-83 (June 1983).

5. Criminal Code R.S.C. 1985, c. C-46, as amended.

6. Copyright Act R.S.C. 1985, c. C-42.

7. Response of the Government of Canada to the Report of the Parliamentary Sub-Committee on Computer Crime, Department of Justice, Canada (October 1983).

8. Bill C-19, the proposed Criminal Law Reform Act, 1984, 2nd Session, 32nd Parliament, 32-33 Elizabeth II, 1983-84.

9. Bill C-18, the proposed Criminal Law Amendment Act, 1984, 1st Session, 32nd Parliament, 33 Elizabeth II, 1984.

10. S.C. 1985, c.19 [now consolidated as R.S.C. 1985, c. C-27 (1st Supp)].

11. Ss. 380-96, para. 326(l)(b), s. 184, ss. 430-31. s. 342 and ss. 366-368, respectively.

12. Sub. 430(1.1); see Appendix "A".

13. Sub. 342.1(1); see Appendix "A".

14. S. 321; see Appendix "A".

15. Ibid.

16. For an analysis of information theory, see Campbell, Grammatical Man: Information, Entropy, Language and Life (New York, 1982). See also: Hammond, "Quantum Physics, Econometric Models and Property Rights to Information" 27 McGill L. Rev. 47 (1981); and Hammond, "Theft of Information", 100 L.Q.R. 252 (1984).

17. For example, the arrangement of the following four letters of the alphabet, "o,p,r,u", as follows, "pour", may represent a concept in the English language meaning "to emit in a stream; to cause a liquid or granular substance to flow out of a vessel or receptacle; to discharge copiously"; or, it may represent a concept in the French language equivalent to the English preposition "for": The Oxford English Shorter Dictionary (3rd) (Oxford, 1980); Harrap's Shorter Dictionnaire - Dictionary (London, 1982).

    Even within the same language, the same alphabetic characters "a,b,e,r" arranged as "bear" may have different meanings: as a noun, "a heavily-built, thick-furred plantigrade quadruped, of the genus Ursus, belonging to the carnivora, but having teeth partly adopted to a vegetable diet", or, as a verb, "to sustain, support; to sustain successfully; to sustain anything painful or trying; to endure,

to tolerate; to hold up, hold on top or aloft": The Oxford Shorter Dictionary, supra.

18. Sub. 342.1(2); see Appendix "A".

19. See a discussion of these problems in Chapter III of the report of the Organization for Economic Co-operation and Development on computer-related criminality entitled, Computer-Related Crime: Analysis of Legal Policy (Paris, 1986).

20. Although the general definition of "property" in s. 2 of the Criminal Code includes intangibles such as a bank deposit credit, the term "property" for the purpose of Part XI, concerning criminal damage to property, is defined in s. 429 as "real or personal corporeal property".

21. Para. 430(1)(a): Everyone one commits mischief who wilfully "destroys or damages property".

22. Example: Austria, Belgium, Canada, Denmark, Finland, Germany, Greece, Italy, Norway and the United Kingdom.

23. Note the distinction between "information" and "data" discussed earlier.

24. Ss. 433-436.

25. Example: para. 430(1)(b): "renders property dangerous, useless, inoperative or ineffective".

26. See infra.

27. S. 430(1.1); see Appendix "A".

28. Para. 430(1)(c) and (d): "(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property, or (d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property."

29. Example: Regina v. Christensen (1978), 26 Chitty's L.J. 348 (Alta. S.C.).

30. Example: Belgium, Canada, Denmark, Germany, Greece, Italy, Norway and the United Kingdom.

31. (1984), 13 C.C.C.(3d) 430 (Ont. H.C.J.); and see supra, note 28.

32. Sub. 430(1.1); see Appendix "A".

33. Para. 430(1.1)(a); see Appendix "A".

34. See Appendix "A".

35. Sub. 342.1(2); see Appendix "A".

36. Sub. 430(1.1); see Appendix "A".

37. Sub. 429(1) extends the definition of "wilfully" to include subjective recklessness.

38. Example: Italian Penal Code, s. 617; German Penal Code, s. 201; Penal Code of the Netherlands, ss. 139a, 139c; Swiss Penal Code, s. 179 bis; United States Federal Wire Tap Act, and title III of the Omnibus Crime Control and Safe Streets Act of 1968, para. 2510-2520.

39. Para. 326(1)(b), Criminal Code.

40. S. 184, Criminal Code.

41. Ibid.

42. Although s.2 of the Criminal Code (definition of "every one", "person" and "owner") and the Interpretation Act, R.S.C. 19850, c. I-21, s.35, define "person" to include corporate entities, the majority of the Court in R. v. Davie (1981), 54 C.C.C. (2d) 216, at 223, 2 W.W.R. 513, at 521 (B.C.C.A.) held that, for the purposes of s. 178.1 (now. s. 183) of the Criminal Code, which defines "private communication", "person" refers to "'a human being...having rights or duties recognized by law'". See also Bellemare, Chronique, 39 R. Du B. 1102 (1979).

43. Interpretation Act, R.S.C. 1985, c. I-21, s. 35.

44. It is doubtful whether communications in these circumstances constitute either "communication" or "private communication" within the meaning of those terms. The definition of "private communication" in present s. 183 has two components. First, there must exist "any oral communication or any telecommunication". Second, the communication must be "private"; i.e., "made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it". With respect to the first component, controversy has arisen as to whether there must exist a sharing or exchange of ideas, knowledge or information between more than one person in order to constitute a "communication" or whether the imparting of ideas, knowledge or information by one originator is sufficient. Controversy has also surrounded the second component as to whether in order to constitute a "private communication", there must exist a "person intended by the originator thereof to receive" the communication or whether an expectation of privacy in the mind of the originator is sufficient. See also Goldman v. The Queen, [1980] 1 S.C.R. 976, 108 D.L.R. (3d) 12 (1979); R. v. Davie, supra note 20; D. Bellemare, L'ecoute Electronique au Canada 217 (1981); D. Watt, Law of Electronic Surveillance in Canada (1983).

45. See Appendix 'A'.

46. Sub. 353.1(2); see Appendix 'A'.

47. It is the interception of a function of that system, rather than the interception of the data itself that is prohibited by paragraph 342.1(1)(b). Arguably, no interception takes place in respect of stored data unless it is being communicated at the time of interception or unless, through the perpetrator's own actions, the data is caused to be communicated and this function of the computer system is thereby intercepted and the data acquired by the perpetrator.

48. Example: The Danish Penal Code, as amended in 1985, section 263; Swedish Data Act (1973), section 21; United States Access Device and Computer Fraud and Abuse Act (1984) only refers to "access".

49. Acquisition of the data, however, may permit the acquirer to decipher, interpret or understand its informational content.

50. Section 184.

51. In Malone v. Metropolitan Police Comm'r, [1979] Ch. 344, at 357, [1979] 2 W.L.R. 700, at 711, the plaintiff (who sought declaratory relief in respect of the wiretapping of his telephone by the police) argued that to "tap a person's telephone conversation without his consent...was unlawful because that person had rights of property in his words as transmitted by the electrical impulses of the telephone system, and so the tapping constituted an interference with his property rights". Megarry V.C., id. at 357, [1979] 2 W.L.R. at 711-12, held that he did "not see how words being transmitted by electrical impulses could themselves (as distinct from any copyright in them) fairly be said to be the subject matter of property".

52. Example: Germany, Norway.

53. Example: Canada, France.

54. Sub. 342.1(1); see Appendix 'A'.

55. The Canadian policy with respect to this offence is that an infringement of security measures is not a prerequisite to criminal liability. It is the state of mind of the accused that is important. A person should be guilty if that person lacks any honest belief that he or she had a right to do what was done, regardless of the degree of security that may exist. The degree of security, however, may effect the belief of the accused, or the court's acceptance that the person truly and honestly held that belief. For example, if a person had to break a complex security system, that person would likely lack the possession of a colour of right. On the other hand, even if there were no security system, but the person knew that he or she had no right, they would again be liable. While it is recognized that an effort to maintain secrecy is a proper requirement for trade secret law (since it distinguishes the type of information which is to be protected and which can be the subject of theft), security measures are not independently important in their own right with respect to entry and surveillance. As an analogy, it is an offence to open the door of a house, enter and steal personal property regardless of the degree of security implemented by the owner. It is also unlawful to trespass on real property (land) even if there is no security. Once access is gained, if the thing to be appropriated is information (e.g. a trade secret), the presence or absence of security measures, on the other hand, would be important as it would, along with other criteria (e.g., business or trade purpose), define the type of information that is subject to legal protection.

56. Example: State v. McGraw, 459 N.E. 2d 61 (Ind. App., 2d Dist 1984); contra People v. Weg, 113 Misc. 2d 1017, 450 N.Y.S. 2d 957 (Crim. Ct. 1982).

57. Example: Austrian Penal Code, section 149(2); German Penal Code, section 256(a); Swiss Penal Code, sections 150, 151.

58. In R. v. McLaughlin, supra note 13, the Supreme Court of Canada held that a computer did not constitute a "telecommunication facility". Its primary function was data processing, not transmission of telecommunications, to which para. 287(1)(b) [now para. 326(1)(b)] was primarily directed.

59. Example: Canadian Criminal Code, section 326(1)(a); French Penal Code, section 379; United Kingdom Theft Act, section 13.

60. Example: German Penal Code, section 2486.

61. Example: R. v. Marine Resource Analysts Ltd. (1980), 41 N.S.R. (2d) 631 (Co. Ct.).

62. The "advantage" to the personator within the meaning of sub. 403(a), or "disadvantage" to the other person within the meaning of sub. 403(c) is not restricted to pecuniary or economic terms: R. v. Hetsberger (1980), 51 C.C.C. (2d) 257 (Ont. C.A.); Rozon v. The Queen (1974) 28 C.R.N.S. 232 (Que. C.A.). See also Finlay, "Another Alternative: Personation", 1 Can. Computer L.R. 70 (1984).

63. Supra, note 56.

64. See George, "Contemporary Legislation Governing Computer Crimes", 21 Crim. L. Bultn 389 (1985).

65. Para. 342.1(1)(a); see Appendix 'A'.

66. Example: Austria, Portugal; see note 19, supra.

67. Example: Belgian Penal Code, section 461; Danish Penal Code, section 293.

68. Example: Austria, Canada, Germany, Netherlands.

69. Example: Norway, Switzerland.

70. Proposals have been made in Finland, Norway and Sweden; see note 19, supra.

71. Para. 342.1(1)(c); and see supra, note 64.

72. Example: California Penal Code, section 502.

73. Example: United States Electronic Fund Transfer Act, section 1693.

74. S. 342.1; see Appendix 'A'.

75. Para. 342.1(1)(c); see Appendix 'A'.

76. However, some American states punish simple access (i.e. use) if done intentionally and knowingly without authorization; e.g. California. See supra, note 64 at p. 405n.

77. In Arizona, Colorado, Minnesota, Utah and Virginia, unauthorized access is not a crime unless some further intent or consequence other than intentional access is present: see supra, note 64 at p. 406n. See also Report on Computer Crime, Scottish Law Reform Commission, No. 106.

78. In Canada, some breaches of copyright have also been held to constitute the criminal offence of fraud. In R. v. Kirkwood (1983), 35 C.R. (3d) 97 (Ont. C.A.) the accused, who sold and rented videotapes that had been unlawfully duplicated, was convicted of defrauding the holder of the copyright despite the absence of deceit, falsehood or a relationship between the accused and the holder of the copyright. The dishonest acts (knowingly acting in breach of copyright) constituted "other fraudulent means" within the meaning of the statute, and caused both actual and a risk of prejudice to the economic interests of the owner of the distribution rights and copyright. This dishonest deprivation constituted fraud.

79. Given the distinction between "information" and "data", it is conceivable that a person can acquire data without acquiring (deciphering or understanding) its information content.

80. Example: Oxford v. Moss [1979] Cr. App. R. 183; Regina v. Stewart (1988), 41. C.C.C. (3d) 481; 63 C.R. (3d) 305; and see the report of the Scottish Law Commission, Report on Computer Crime, Scot Law Com No. 106, Edinburgh; Contra.

81. Chambre Criminelle de la Cour de Cassation, decision of 8th January 1979.

82. Arnhem Court of Appeals, decision of 27 October, 1983.

83. Example: U.S. v. Bottone, 365 F. 2d 389 (1966); U.S. v. Lambert, 446 F. Supp. 890 (1978); United States v. Girard, 601 F 2d 69 (2d Cir. 1979); United States v. Sampson, 507 F. Supp. 495 (E.D. Pa. 1981).

84. U.S. v. Bottone, supra, note 83, at p. 393-94.

85. Example: Ward v. Superior Court, 3 Computer L. Serv. Rep. 206 (Calf. 1972); Commonwealth v. Yourawski, 425 N.E. 2d 298 (Mass. 1981).

86. Carpenter v. U.S. (1987), 42 Crim. L.R. 3009 at 3011-12. See criticism of Carpenter in: Coffee, "Hush!: The Criminal Status of Confidential Information After McNally and Carpenter and the Enduring Problem of Overcriminalization" (1988), 26 Am. Crim. L. Rev. 121.

87. Supra, note 80.

88. Regina v. Stewart (1983), 42 O.R. (2d) 225, 35 C.R. (3d) 105 (Ont. C.A.). The scope of this article does not permit an analysis of this decision. In this regard, see Hammond, "Theft of Information", 100 L.Q.R. 252 (1984) and Magnusson,

"Kirkwood and Stewart: Using the Criminal Law Against Infringement of Copyright and the Taking of Confidential Information". 35 C.R. (3d) 129 (1983).

89. Supra, note 80.

90. Some of the concerns raised by various reports and commentators, and discussed by the Court included the following issues. To provide that the unauthorized acquisition of information would constitute the offence of theft raises broad policy implications. For example, the civil breach of copyright or patent, or the glancing and acquisition of the contents of a letter lying on someone else's desk, even without any form of physical contact, might also constitute "theft" or "conversion". Innocent third party acquirers of information, who subsequently learned of the stolen nature of the information, could be put into a perpetual state of criminality by their possession where laws punish possession of stolen property as opposed to just receipt of such. Treating information as property for criminal law purposes might also adversely effect employer-employee relations and the mobility of labour by restricting former employees from using confidential information that was acquired in the course of employment with the former employer. The law of theft also does not provide the required balance, in terms of defences, to accommodate the interests of third party acquirers or disclosures made in the public interest. The property concept may not provide for the needed degree of flexibility and balance between, on one hand, the protection of information and, on the other hand, a free flow of information.

At the legislative level, concerns were also expressed. The Canadian Parliamentary Sub-Committee on Computer Crime stated that Parliament would be ill-advised to try to protect information by granting a proprietary interest in it. "For reasons of public policy, the exclusive ownership of information, which, of necessity, would flow from the concept of 'property' is not favoured in our socio-legal system. Information is regarded as too valuable a public commodity to have its ownership vest exclusively in any particular individual": supra note 4, at para. 29. The Sub-Committee recommended instead that a joint federal-provincial study be undertaken concerning trade secrecy laws with a view to developing federal and provincial legislation directed at the misappropriation of information. See also Hammond, "Quantum Physics, Econometric Models and Property Rights to Information", 27 McGill L.J. 47 (1981); Alberta Institute of Law Research and Reform, Improper Interference With Computers And The Misappropriation Of Commercial Information, Background Paper (1983), written in conjunction with the Department of Justice, Canada.

D-36

91. Supra, note 80, at p. 317 (C.R.).

92. In favour of ascribing property status to information, see: Weinrib, "Information and Property" (1988), 38 U.T. L.J. 117; Doherty, "Stewart: When is a thief not a thief? When he steals the 'candy' but leaves the 'wrapper'." (1988), 63 C.R. (3d) 322. Critical of ascribing property status to information, see: R. v. Offley (1986), 51 C.R. (3d) 378, 28 C.C.C. (3d) 1 (Alta. C.A.); Hayhurst, Note (1983) 12 Eur. Intell. Prop. Rev. 261; Hammond, "Election Crime in Canadian Courts" (1986), 6 Oxford J. of Legal Studies 145; Hammond, "The Misappropriation of Commercial Information in the Computer Age" (1986), 64 Can . Bar Rev. 342; Hammond, "Theft of Information" (1984), 100 Law Q.R. 252; Webber, "Computer Crime or Jay-Walking on the Electronic Highway" (1983), 26 Crim. L.Q. 217; Roberts, "Is Information Property?" (1987), Intell. Prop. J. 209.

93. This distribution was recognized by the federal-provincial report on Trade Secrets, Report No. 46, July 1986, of the Institute of Law Research and Reform of Alberta.

94. Per Lacourcière J.A., in the decision of the Ontario Court of Appeal, as quoted and adopted by the Supreme Court of Canada, at p. 496-97 (C.C.C.).

95. For example, see George, "Contemporary Legislation Governing Computer Crimes", 21 Crim. L. Bultn 389 at 401n (1985).

96. Supra, note 4, at para. 31.

97. Eisenberg, "Proprietary Rights and the Norms of Science in Biotechnology Research" (1987), 97 Yale L.J. 177; Korn, "Patent and Trade Secret Protection in University-Industry Research Relationships in Biotechnology" (1987), 24 Harvard J. on Legislation 191; Pollack, "Patent Litigation New Revenue Source for Firms in U.S.", Globe and Mail July 9, 1989, p. B17; "Drugs Need New Boffins", The Economist, July 16, 1989, p. 15; Coffee, "Hush!: The Criminal Status of Confidential Information After McNally and Carpenter and the Enduring Problem of Overcriminalization", (1988), 26 Am. Crim. L. Rev. 121.

98. Hammond, "Quantum Physics, Econometric Models and Property Rights to Information", 27 McGill Law Journal 47 (1981).

99. Supra, note 4, at para. 29; see also note 90, supra.

100. Supra, note 93.

101. Example: Finland, Germany and Sweden.

102. See the work of the Commissioners on Uniform State Laws: Uniform Trade Secrets Act, 14 U.L.A. 539-51 (1980).

103. In this regard, it should be noted that the new Canadian amendments do not contain any provisions amending the definition of "property" so as to include "information" or "computer-stored information" so that the existing theft and fraud provisions of the Criminal Code might apply. The protection of computerized information from misappropriation is to be achieved via the offences of, dishonestly and without a colour of right, (a) obtaining a computer service, (b) intercepting a function of a computer system and (c) using a computer system with the prescribed mental intentions.

104. Computer-Related Crime: Analysis of Legal Policy, Organization for Economic Cooperation and Development (Paris, 1986); Report of the European Committee on Crime Problems on Computer-Related Crime, Council of Europe (to be published in 1989).

APPENDIX 'A'

The following is the text of the amendments to the Criminal Code R.S.C. 1985, c. C-46 (hereinafter referred to as the "Act"), concerning computer-related criminality, as re-enacted by R.S.C. 1985 c. C-27 (1st Supp).

42. The definition "document" in section 321 of the said Act is repealed and the following substituted therefor:

"credit card" *«carte...»*

" "credit card" means any card, plate, coupon book or other device issued or otherwise distributed for the purpose of being used

(*a*) on presentation to obtain, on credit, money, goods, services or any other thing of value, or

(*b*) in an automated teller machine, a remote service unit or a similar automated banking device to obtain any of the services offered through the machine, unit or device;

"document" *«document»*

"document" means any paper, parchment or other material on which is recorded or marked anything that is capable of being read or understood by a person, computer system or other device, and includes a credit card, but does not include trademarks on articles of commerce or inscriptions on stone or metal or other like material;"

42. La définition de «document» à l'article 321 de la même loi est abrogée et remplacée par ce qui suit :

«carte de crédit» *"credit..."*

«carte de crédit» Désigne notamment les cartes, plaquettes ou coupons délivrés afin :

a) soit de procurer à crédit, sur présentation, des fonds, des marchandises, des services ou toute autre chose de valeur;

b) soit de permettre l'accès, par un guichet automatique, un terminal d'un système décentralisé ou un autre service bancaire automatique, aux différents services qu'offrent ces appareils.

«document» *"document"*

«document» Papier, parchemin ou autre matière sur lesquels est enregistré ou marqué quelque chose qui peut être lu ou compris par une personne, un ordinateur ou un autre dispositif, y compris une carte de crédit. La présente définition exclut toutefois les marques de commerce sur des articles de commerce et les inscriptions sur la pierre ou le métal ou autre matière semblable.»

Unauthorized use of computer

"**342.1** (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, or

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Utilisation non autorisée d'ordinateur

«**342.1** (1) Quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;

b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa *a*) ou *b*) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur,

est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Definitions

(2) In this section,

"computer program" *«programme...»*

"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" *«service...»*

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

"computer system" *«ordinateur»*

"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" *«données»*

"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;

"electro-magnetic, acoustic, mechanical or other device" *«dispositif...»*

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

"function" *«fonction»*

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

"intercept" *«intercepter»*

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

Définitions

(2) Les définitions qui suivent s'appliquent au présent article.

«dispositif électromagnétique, acoustique, mécanique ou autre» *"electro-magnetic..."*

«dispositif électromagnétique, acoustique, mécanique ou autre» Tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une fonction d'un ordinateur, à l'exclusion d'un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale.

«données» *"data"*

«données» Représentations d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur.

«fonction» *"function"*

«fonction» S'entend notamment des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé des données de même que des fonctions de communication ou de télécommunication de données à destination, à partir d'un ordinateur ou à l'intérieur de celui-ci.

«intercepter» *"intercept"*

«intercepter» S'entend notamment du fait d'écouter ou d'enregistrer une fonction d'un ordinateur ou de prendre connaissance de sa substance, de son sens ou de son objet.

«ordinateur» *"computer system"*

«ordinateur» Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux :

a) contiennent des programmes d'ordinateur ou d'autres données;

b) conformément à des programmes d'ordinateur :

(i) soit exécutent des fonctions logiques et de commande,

(ii) soit peuvent exécuter toute autre fonction.

«programme d'ordinateur» *"computer program"*

«programme d'ordinateur» Ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction.

«service d'ordinateur» *"computer service"*

«service d'ordinateur» S'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données.»

57. (1) Section 430 of the said Act is amended by adding thereto, immediately after subsection (1) thereof, the following subsection:

57. (1) L'article 430 de la même loi est modifié par insertion, après le paragraphe (1), de ce qui suit :

Mischief in relation to data

"(1.1) Every one commits mischief who wilfully

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data; or

(*d*) obstructs, 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."

Méfait concernant des données

«(1.1) Commet un méfait quiconque volontairement, selon le cas :

a) détruit ou modifie des données;

b) dépouille des données de leur sens, les rend inutiles ou inopérantes;

c) empêche, interrompt ou gêne l'emploi légitime des données;

d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit.»

(2) Subsections 430(3) to (5) of the said Act are repealed and the following substituted therefor:

(2) Les paragraphes 430(3) à (5) de la même loi sont abrogés et remplacés par ce qui suit :

Idem

"(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds one thousand dollars

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(*b*) is guilty of an offence punishable on summary conviction.

Idem

«(3) Quiconque commet un méfait à l'égard d'un bien qui constitue un titre testamentaire ou dont la valeur dépasse mille dollars est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de dix ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Idem

(4) Every one who commits mischief in relation to property, other than property described in subsection (3),

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(*b*) is guilty of an offence punishable on summary conviction.

Idem

(4) Quiconque commet un méfait à l'égard d'un bien, autre qu'un bien visé au paragraphe (3), est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Idem

(5) Every one who commits mischief in relation to data

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(*b*) is guilty of an offence punishable on summary conviction.

Idem

(5) Quiconque commet un méfait à l'égard de données est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de dix ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Offence

(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(*b*) is guilty of an offence punishable on summary conviction."

Infraction

(5.1) Quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de cinq ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.»

(3) Section 430 of the said Act is further amended by adding thereto the following subsection:

(3) L'article 430 de la même loi est modifié par adjonction de ce qui suit :

Definition of "data"

"(8) In this section, "data" has the same meaning as in section 342.1."

Définition de «données»

«(8) Au présent article, «données» s'entend au sens de l'article 342.1.»

CURRICULUM VITAE

PERSONAL DATA

Name:	Donald Kenneth Piragoff
Professional Address:	Department of Justice Room 722 239 Wellington Street Ottawa, Ontario K1A 0H8
Telephone:	(613) 957-4730
Professional Status:	June 28, 1979, admitted and enrolled a Barrister and Solicitor of the Court of Queen's Bench for the Province of Manitoba

ACADEMIC RECORD

University Education

Universities Attended	Academic Years	Faculty	Degree
University of Winnipeg	1972-1975	Major: Political Science; Sociology Minor: Philosophy	B.A.

Universities Attended	Academic Years	Faculty	Degree
University of Manitoba	1975-1978	Law	LL.B.
University of Toronto	1979-1980	Law	LL.M.

DH2

Particulars of Graduate Studies

My LL.M. thesis was in the area of criminal law and evidence (specifically, similar fact evidence), and was completed under the supervision of Professor A.W. Mewett, (pages: 480). During this period, I also studied Evidence under Sir Rupert Cross, late Vinerian Professor of Law, Oxford.

Scholarships, Prizes, Distinctions, Awards

April 1979	Duff-RinfretScholarship (Department of Justice, Canada)
March 1979	University of Toronto Fellowship in Law (declined)
May 1978	The Alf Francis Memorial Prize (for third highest standing; Third Year Law)
	The Law Society of Manitoba Prize (for third highest standing; Third Year Law)
	University of Manitoba, Faculty of Law, Dean's Honour List
December 1977	The Hart Green Junior Memorial Prize in Criminal Procedure
May 1975	University of Winnipeg, Dean's Honour List: Student of Highest Distinction
	The University Gold Medal
October 1974	The Board of Regents General Proficiency Scholarship
May 1974	University of Winnipeg, Dean's Honour List: Student of Highest Distinction

October 1973	The D.J. Jessiman Scholarship in Political Science
	The Winnipeg RH Institute Inc. General Proficiency Scholarship
	The Lorne Elliot Scholarship in Sociology
May 1973	University of Winnipeg, Dean's Honour List: Student of Highest Distinction

Professional Experience

November 1988 to present	Acting General Counsel/Director Criminal Law Policy Section Department of Justice, Ottawa
April 1987 to present	Senior Counsel Criminal Law Policy Section Department of Justice, Ottawa
June 1981 to April 1987	Counsel, Criminal Law Policy and Amendments Department of Justice, Ottawa
July 1980 to May 1981	Lecturer, Osgoode Hall Law School York University, Toronto
September 1979 to May 1981	Legal Consultant: Walsh, Micay and Company; and, Gindin, Soronow and Malamud, Winnipeg, Manitoba
September 1979 to August 1980	Research Assistant, Faculty of Law University of Toronto
May 1978 to June 1979	Articled-Clerk-at-Law, Walsh, Micay & Company, Manitoba, under articles to Harry Walsh, Q.C., and G. Gregory Brodsky, Q.C.

D44

Major Publications

Similar Fact Evidence, Carswell Company Limited, Toronto, 1981 (pages: 309)

"Bill C-19: Reforming the Criminal Law; Computers" (1984), 16 Ottawa Law Review 306

"Les projets législatifs canadiens visant à la protection de l'intégrité des systèmes informatiques" (1985) Droit de l'informatique 33

"Combatting Computer Crime with Criminal Laws", in Computermisdaad en Strafrecht (ed.), H.W.K. Kaspersen, Kluwer rechtswetenschappen, Antwerpen, Belgie (1986), at 103

D45