January 1987

Recent Amendments to the Canadian Criminal Code Respecting Computer Abuse Offenses

Chris Webber

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

Chris Webber, Recent Amendments to the Canadian Criminal Code Respecting Computer Abuse Offenses, 3 SANTA CLARA HIGH TECH. L.J. 165 (1987).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol3/iss1/7

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
I. INTRODUCTION

On April 24, 1985, Bill C-18, The Criminal Law Amendment Act, 1985, was passed into law by the House of Commons of Canada. The Act amended the Criminal Code by introducing, among other things, specific sections relating to computer abuse offenses. As a result, Canadian law enforcement agencies can now lay charges for criminal activities involving computers which had been conspicuously missing from the Criminal Code. United States companies doing business in Canada can now rely on the Criminal Code to deter those in Canada who would invade their computer systems or destroy or alter data stored in their computers.

In order to understand the full significance of the recent amendments to the Criminal Code, in addition to analyzing the new sections, one must examine the circumstances which have led to such changes. Also, recent case law and current proposals for other laws which incorporate penal sections for offenses involving computers should be examined.

This paper will examine the new language of the Criminal Code for computer related offenses and will discuss some of the definitional problems which are unavoidable when dealing with such matters. Relevant cases will also be reviewed in order to fully comprehend their present and future effect on this area of the law. Unlike the United States where most criminal laws are within the jurisdiction of each state, Canadian criminal matters are under the...
exclusive authority of the federal government. To better understand the similarities and differences between Canadian computer-related criminal laws and United States legislation, the new provisions of the Canadian Criminal Code will be compared with the corresponding sections of the California Penal Code, which is one of the leading jurisdictions in the United States regarding computer offense statutes.

The new provisions in the Criminal Code and the corresponding cases relating to computer abuses and misappropriation of proprietary information will act as the foundation for future Canadian legislative changes. It is of utmost importance that such laws are built upon a sound conceptual base.

II. THE INSPIRATION FOR CHANGE: R. v. MCLAUGHLIN

The relevant sections of the amended Criminal Code are Sections 301.2 and 387(1.1), both of which were passed in response to the issues raised by the Supreme Court of Canada in the case of R. v. McLaughlin.

McLaughlin was convicted at trial on a charge that he “fraudulently, and without colour of right, used a telecommunication facility, the property of the University of Alberta, contrary to Section 287(1)(b) . . . of the Criminal Code.” McLaughlin was a University of Alberta student who had gained access to certain computer security codes which enabled him to obtain the identity and secret passwords of other users. When apprehended by the police, he admitted that he had examined the computer files of public users and had made changes in the billings of other accounts.

The Alberta Court of Appeal permitted his appeal and the conviction was quashed. In 1980, that decision was upheld by the Supreme Court of Canada.

The primary issue before the Supreme Court was whether the appropriation of the programs (and other information) involved use of a telecommunication facility, as referred to in Section 287(1)(b) and as defined in Section 287(2) of the Criminal Code. Section 287 states:

287. (1) Every one commits theft who fraudulently, maliciously, or without colour of right,
Chief Justice Laskin, in his decision for the majority of the Supreme Court, found that a computer system may be termed a facility. However, he reasoned that its function was not transmission as required under section 287(2). According to Laskin:

"The function of the computer is not the channeling of information to outside recipients so as to be susceptible in that respect to unauthorized use. Rather, it is to permit the making of complex calculations, to process and correlate information and to store it, and to enable it to be retrieved. The distinction I would draw is admittedly, narrow. However, I do not think that using a terminal, as did the accused . . . brings such use within § 287(1)(b) . . . The fact that the accused, by using the terminal, was able to make electronic connection with the central processing unit to capture information that was stored there does not advance the case against him." 7

In reaching its decision, the court did not have to address the issue of whether the information appropriated constituted an offense against rights of property as defined in Part VII of the Criminal Code under the general provisions for Theft. Specifically, in Part VII, Section 283(1) establishes that the object of a theft is "anything whether animate or inanimate."

As Linda Whan pointed out in her case comment Computer Crime and R. v. McLaughlin: "This issue arises out of the fact that data on a computer printout or tape is an intangible." 8 The fundamental problem involves ascertaining whether there are proprietary rights attachable to such intangibles as computer programs or data stored in computers. The Supreme Court of Canada concluded in McLaughlin that the Criminal Code ought to specifically relate to unauthorized access to computer facilities before the courts should convict an individual for such conduct. 9

The impact of the McLaughlin case was not taken lightly by

7. Supra note 4, 113 D.L.R.3d, at 390 (1980).
9. See the judgment of Estey J. in McLaughlin, supra note 4, 113 D.L.R.3d, at 394,
those concerned with computer abuse. Shortly after the decision was handed down, the Canadian Bar Association (CBA) sent a telegram to the then Justice Minister Jean Chretien and all Attorneys-General and Territorial Legal Officers requesting that immediate steps be taken to resolve the problem. Cosigning the telegram were the Canadian Information Processing Society (CIPS) and the Canadian Law Information Council (CLIC), two of the more prominent institutions representing the electronic data processing profession.

At that time Gordon Henderson, President of the CBA, called for an immediate revision of the Criminal Code to define a computer as a telecommunication device. However, Silas Halyk, Canadian Law Information Council's Chairman, and Gaylen Duncan, an associated computer law expert and editor of the CIPS Review, both voiced the need for a more tempered approach. Both recommended in-depth studies of the implications and consequences of the McLaughlin case.

Around the time of McLaughlin, another computer-abuse incident received a great deal of media attention and again illustrated the need for effective revisions to curb computer abuses. In April of 1980, youthful pranksters in the exclusive Dalton private school in Manhattan used the school's terminal to attempt to penetrate and vandalize twenty-one Canadian computer systems. The Royal Canadian Mounted Police (RCMP), the Federal Bureau of Investigation (FBI) and Bell Canada investigated a complaint from a Montreal cement company which detected unauthorized attempts to access their system. The youths had found a link between Bell Canada's Datapac and GTE Telenet Communications Corporation of Vienna, Virginia through which they were able to tap into systems owned by Bell Canada, Honeywell Ltd., Concordia University, the universities of Waterloo and Alberta, and others.

Some of the owners involved in the investigation were completely unaware that their computer had been accessed, while in other situations the youths had destroyed information when the system's monitors and security had not allowed them access. This "computer caper" further accentuated the need to prevent and deter such activities.

Over the past ten years, law enforcement agencies have exerted

---

11. See, Computer Fraud was First Spotted at City Company, Montreal Gazette, May 8, 1980, at 7.
commendable efforts to keep abreast of the issues. The RCMP created an Electronic Data Processing (EDP) Security Section in the Security Systems Branch in Ottawa. The section has developed training courses in computer crime and has trained squads of specialists who have been posted in various divisions throughout the country.\textsuperscript{12} The Provincial Police have also responded by creating special "fraud squads" to combat criminals using computers.

The police were convinced that crimes perpetrated by the use of computers were far more prevalent than statistics indicated. Law enforcement agencies were in a frustrating situation; special forces had been devised to investigate and apprehend computer criminals, but the courts refused to convict them under the Criminal Code.

III. THE EVOLUTION OF THE NEW AMENDMENTS

The new amendments represent the culmination of a number of attempts to draft computer-related offenses for inclusion in the Criminal Code. In February, 1981 Bill C-628 went to First Reading in the Canadian House of Commons.\textsuperscript{13} The Bill was introduced by Mr. Taylor, Member of Parliament, and was intended to provide amendments to the Criminal Code regarding computer-related crimes. That Bill redefined property in Section 2 of the Criminal Code to include "financial instruments, information, electronically produced data, computer software and programs in either machine or human readable form, and any other tangible or intangible item of value."\textsuperscript{14} In Section 283, the definition of "anything" was to be changed to incorporate all of the above mentioned intangibles.\textsuperscript{15} Bill C-628 met with a great deal of resistance and was ultimately defeated, in part, due to its inherent definitional problems.

Bill C-667\textsuperscript{16} was the successor to Bill C-628. It was introduced by another Member of Parliament, Mr. Perrin Beatty, and was given First Reading in Parliament on December 16, 1982. Like its predecessor, C-667 attempted to grapple with the definitional problems concerning computer-related crime. To this end the definition of computer was revised to mean: "... any programmable device or apparatus designed to store processed data or information, but does not include a hand-held calculator or similar device."\textsuperscript{17}

\begin{itemize}
  \item[\textsuperscript{12}] See, Barrett, \textit{Police Taking Special Courses}, Vancouver Sun, Sept. 10, 1980, at 1.
  \item[\textsuperscript{14}] Id. § 1; see also commentary in clause 1 of explanatory notes.
  \item[\textsuperscript{15}] Id.
  \item[\textsuperscript{17}] Id., at Cl. 1.
\end{itemize}
Both of the above mentioned Bills exemplify the inherent problems faced by legislators when drafting laws which propose to regulate the use of computers. Inevitably, the technology will render the legislation antiquated.

Bill C-667 was ultimately withdrawn from Second Reading on February 9, 1983 and its subject-matter was referred to the Standing Committee on Justice and Legal Affairs for further study. The committee subsequently published a report in June, 1983\(^1\) which led to the creation of the Criminal Law Reform Act, 1984 (Bill C-19). Due to the federal election in 1984 and the ultimate change in government, Bill C-19 was not enacted.

IV. PROBLEMS OF DEFINITION

The foregoing brief overview has been provided to demonstrate the amount of effort expended in attempting to define such terms as computer, programming, data and other computer-related terminology. United States legislative draftsmen have experienced similar difficulties when trying to define computer terminology. United States Senate Bill S.240 - Federal Computer Systems Protection Act of 1979\(^1\) came under considerable criticism for its uncertainty and all-encompassing character.\(^2\)

The task, as outlined by John K. Taber, is that of excluding: "...trivia like calculators at one end of the scale, and the telephone system, which is the largest special purpose computer ever built, at the other. The purpose of such an exercise is to limit the definition of computer to a general purpose digital computer used for record keeping."\(^2\) The failure to make such a distinction, says Taber, threatens to make criminals out of the large number of members in the EDP professions.\(^2\)

Subsequent to the criticism received by Bill S.240, another Bill, H.R.3970, was introduced in 1981.\(^2\) This new legislation attempted to plug the apparent gaps in Bill S.240. The broad-sweeping definition of computer was somewhat restricted in the new Bill by excluding: "... an automated typewriter or typesetter, or any

4. Id. at 532, n. 88.
5. See Taber, supra note 20, at 530.
computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes including a portable hand-held electronic calculator." The new draft eliminated some of the possibly absurd results of a broad definition but still did not exculpate over-zealous students who print Snoopy calendars or playful programmers who play computer tick-tac-toe.

In Canada, the amendments have been drafted to be broad enough to encompass future computer technology. Under the recent Act, the definition of electromagnetic, acoustic, mechanical or other device reads as follows: "electromagnetic, acoustic, mechanical or other device means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing." In addition, the definition of computer system has been broadened from previous versions. Recall that in Bill C-667, the term computer was defined to exclude "... hand-held calculator or similar device." The definition of computer system in the amendments does not include such an exclusion for pocket calculators. Presumably, the draftsmen were concerned with the possible evolution of pocket calculator technology. It is conceivable that future designs for pocket calculators could incorporate remote computer accessing capabilities which would then bring such a device under the definition of computer system.

Donald Piragoff, in his paper Computers, has commented:

In designing sanctions for the unauthorized use of a computer system, a major concern must be whether Canadian society wishes to criminalize the mere unauthorized use of a computer. A dilemma, therefore, rises in attempting to legislate in this area. If the legislation is too specific it may be technologically or functionally limited in the type 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.

Now, any person who wilfully presses the cancel button on anyone else's pocket calculator, microwave oven, video cassette re-

24. Id.
25. Bill C-18, supra note 1, Cl. 46.
27. Counsel for the Criminal Law Policy and Amendments Section of the Department of Justice in Canada.
29. Id. at 313.
corder or any other product containing microchip technology could be subject to the criminal sanctions as set out in Section 387(1.1) of the Criminal Code relating to mischief. This absurd result illustrates the definitional difficulties which plague these new sections. It will be left to the Courts to develop reasonable definitional parameters.

V. RELEVANT CASE LAW

To date, the most controversial judicial decision involving the misappropriation of proprietary information is found in the case of R. v. Stewart. Stewart was charged with counseling to commit mischief, fraud and theft relating to a list of 600 employees of a large hotel complex. The data included names, addresses and telephone numbers which were contained in personal files and were also stored in the payroll file of the hotel's computer.

The accused, acting as an agent for a trade union seeking bargaining-unit status, approached a security person at the hotel and offered to pay him for surreptitiously copying the confidential information.

In a dissenting opinion, Lacourciere J.A. addressed the issue of whether confidential information could be the subject of theft. He reasoned that it could not and concurred with the trial judge that: "... it is for Parliament to broaden the criminal definition of the property concept if the needs of modern Canadian society require it." However, Houlden J.A. and Cory J.A., representing the majority decision of the Alberta Court of Appeal, allowed the appeal, set aside the verdict of acquittal and convicted Stewart of counseling to commit theft. Of special significance is the reasoning of Cory J.A. wherein he concluded that the unauthorized use of copyrighted works of a confidential nature constitutes theft as defined in Section 283(1) of the Criminal Code. Confidential information can now be stolen according to the Stewart decision.

Stewart has filed Notice of Appeal to the Supreme Court of Canada.

The decision in Stewart was a marked departure from previous case law and will have a resounding impact on intellectual property
law and on criminal law if the Supreme Court of Canada upholds the decision.

R. Grant Hammond, in his paper *Quantum Physics, Econometric Models and Property Rights to Information*,\(^{34}\) states that:

[T]he most striking characteristic of information is that it does not fit easily into the extended concepts of property.

First, sole ownership is vastly complicated in the case of information. The act of theft is often impossible to detect and difficult to prove. A piece of information can be "owned" by two people at the same time without any denial of conventional benefits of ownership.\(^{35}\)

Hammond argues that what may be required is a conceptual shift from viewing information as property to viewing it as a social resource — comparable to the shift from Newtonian physics to quantum mechanics.

In *Stewart*, the Ontario Court of Appeal made the quantum leap alluded to in the Hammond article without any extensive research or study into the implications of such a conceptual shift.

The *Stewart* case was followed in 1984 by *Re Turner et al And the Queen*.\(^ {36}\) There the Ontario High Court refused an application to quash an order of the Provincial Court, Criminal Division, which committed three co-accused to trial on charges of mischief pursuant to Section 387, which is under Part IX of the Criminal Code, entitled "Willful and Forbidden Acts in Respect of Certain Property."

The accused were alleged to have interfered with and to have altered data stored on computer tapes. The court, relying in part on *Stewart*, construed the definition of property to be the same for Section 385 and Subsection 387(1), which describe the offense of mischief, as the court in *Stewart* defined property for the purposes of Subsection 283(1) relating to theft. In his case comment on *R. v. Turner*,\(^ {37}\) John Finlay criticized the judicial reasoning in *Turner* by pointing out that:

"It should be noted in Section 385 that the definition of property is specifically restricted to those offenses set out in Part IX of the Criminal Code of which the offenses of theft and fraud are not

---

35. Id. at 54 (1981).
contained. Therefore, the offense of mischief is different than that of theft or fraud in that property is given a more restricted meaning for purposes of the offense of mischief.\textsuperscript{38}

If the decision in \textit{Turner} is not reversed on appeal, then for purposes of defining property under the Mischief Section of the Criminal Code, the court may apply the definition of property set out under Part VII relating to theft and fraud. It could be argued that this analysis disregards the distinct definitions of property set out under Part VII and Part IX of the Criminal Code and broadens the scope of the Mischief Section to include activities to which historically the Criminal Code has not applied.

Although the intention of both the \textit{Stewart} and the \textit{Turner} courts may have been to provide stop-gap measures until the Criminal Code was amended to include computer-related crimes, one should be wary of decisions that go beyond the interpretative role of the courts. Criminal laws are of the utmost importance in our society. These laws address the more serious contraventions of the rules of social behavior, and consequently they carry with them severe penalties. The ultimate penalties that society may impose on its members are found under criminal sanctions; the death penalty, a social black-listing by way of criminal record and the deprivation of an individual's freedom by way of incarceration are incorporated into the criminal regime. With this in mind, it is imperative that the process of composing and articulating criminal laws should remain with the appropriate authority: the legislature. There is no room in the criminal process for the subjective imposition of judge-made law.

The issue as to whether confidential business information represents property for purposes of the Criminal Code was also addressed in the case of \textit{Regina v. Tannas}, a 1984 decision of the Court of Queens Bench of Alberta, Judicial District of Calgary.\textsuperscript{39} Tannas was a computer programmer hired by Dome Petroleum Limited to develop computer programs to be used for Dome's data processing operations. When he was hired, he signed an employee agreement which stated that upon leaving the company, he might be required to return all papers and documents relating to the company's business. During his employment, Tannas created a number

\textsuperscript{38} Id. at 224 (1984).

\textsuperscript{39} Regina v. Tannas, November 28, 1984, Court of Queen's Bench, Judicial District of Calgary, per Bracco, J. \textit{See also}, Hertz, \textit{Can a Computer Program Be Stolen?}, 1 COMPUTER LAW RPRTR. No. 11, at 85-88 (November 1984).
of specialized computer programs and supervised and assisted in the
development of many others.

When Tannas left Dome, he took with him computer tapes and
hard copies of more than one hundred of Dome's programs alleg-
edly worth between $250,000.00 and $360,000.00.\textsuperscript{40} Many of the
programs taken by Tannas had been developed by him during his
employment, but some were programs in which he had no input
whatsoever. Tannas, when he left Dome, was not given an exit
interview.

The programmer was charged, pursuant to Section 283(1)(d) of
the Criminal Code,\textsuperscript{41} with theft of computer software. Specifically,
it was alleged that Tannas took the computer software with the in-
tent to destroy its confidentiality. In its arguments against Tannas,
the Crown relied heavily on the Stewart case to establish that con-
didential information could be stolen.

In his case comment on the Tannas case, Allen Hertz states
that the judge instructed the jury as follows: "...[T]he courts have
had some difficulty deciding whether the information stored and
used in a computer is anything capable of being converted as con-
templated by the Criminal Code."\textsuperscript{42} Hertz further points out that
the jurors were instructed by the judge that the term anything, as
set out in the Theft Section of the Criminal Code, includes: "...[A]
computer program; and the information contained in a computer
program."\textsuperscript{43}

Ultimately then, the issue for the jury was whether Tannas had
the requisite criminal intent to bring him under Section 283(1)(d).
That is, had Tannas: (a) acted fraudulently, without color of right;
and (b) had he converted Dome's programs with intent to deal with
them in such a manner that they could not be restored to the condi-
tion in which they had been at the time they were converted. The

\textsuperscript{40} Hertz, supra note 39, at 86 (1984).
\textsuperscript{41} Section 283(1) provides as follows:

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

\textsuperscript{42} Hertz, supra note 39, at 87 (1984).
\textsuperscript{43} Id.
Crown was unable to establish beyond a reasonable doubt that Tannas had known that the programs were confidential. Further, Dome had never asked Tannas for the return of any software he may have copied. Thus the jury found Tannas not guilty.

In attempting to obtain a conviction against Tannas, the Crown had also relied on the reasoning of *R. v. Kirkwood* in which the owner of an electronics company was charged with and convicted of fraud under Section 338 of the Criminal Code.44 Kirkwood’s company, Electronic Sight and Sound Centers Ltd., allegedly sold and rented video tapes, which Kirkwood knew had been copied, without obtaining the copyright or distribution rights. The company had created counterfeit tapes from legitimate tapes, many of which had not yet been released to the public in video cassette form. These tapes were made for sale in the company’s outlets along with legitimate tapes. In his decision, Lacourciere J.A., stated that:

> It is conceded by the respondent that while there was no evidence of “deceit” or “falsehood” in relation to the owners, there was evidence to support a finding of dishonesty by “other fraudulent means”. In addition, the respondent conceded that the evidence permits an inference to be drawn that the owners of the copyright and distribution rights were actually or potentially deprived of revenues by the respondent’s conduct. . . . Some form of relationship or nexus between the perpetrator of the fraud and its victim may be necessary in cases where the fraud has been accomplished by deceit or falsehood. However, two essential elements of fraud are “dishonesty” and “deprivation”, the latter element being satisfied on proof of detriment, prejudice or risk of prejudice to the economic interests of the victim.45

Finding against the defendant, the court referred to the 1978 case of *R. v. Olan, Hudson and Hartnett*, a decision of the Supreme Court of Canada, where the judges held that there need not be a nexus between the person committing the fraud and the victim.46

The cases above demonstrate the fact that issues relating to computer technology are causing a conceptual convergence of the criminal law, intellectual and property law, and civil law.

One must query whether the criminal law is the appropriate judicial vehicle to deal with certain aspects of computer-related abuses or misappropriation of proprietary information. This issue is

particularly relevant when considering the apparent overlap of the Copyright Act and the imposition of criminal sanctions relating to proprietary rights in information as imposed by the Stewart and Kirkwood cases. In his review of these two cases, Denis Magnusson, Dean, Faculty of Law, Queens University, commented:

Calls for new criminal sanctions have been made notwithstanding the well-established civil remedies for infringement of copyright (in respect of the type of infringement which occurred in Kirkwood, see the Copyright Act, Section 17(4)) and for the wrongful taking of confidential information or trade secrets. Many would argue that the economic interests of the country as a whole would be served better by the imposition of criminal sanctions for infringement of copyright and the taking of confidential information. However, it should be noted that the Copyright Act presently imposes penal sanctions for infringement of copyright. Unfortunately, the penalties have not been changed since the Act's inception in 1924. Presently, the maximum monetary penalty under the Act is a fine of $200.00 for a first offense.

Was the Stewart decision needed to protect those who maintain proprietary interests in information? According to R. Grant Hammond, it was not. With reference to the Stewart case, Hammond argues:

The decision is open to criticism on three major grounds. It is an example of unwarranted judicial activism which is at odds with certain law reform and parliamentary initiatives in Canada, the technical handling of the authorities relied upon by the majority judgments is suspect, and the practical consequences of the decision are far reaching and do not seem to have been adequately addressed. In his paper, Hammond was very critical of decisions such as Stewart where the judges have taken it upon themselves to reformulate "...long standing, principled statutory policies without challenge or debate". It is interesting to note that at the time the Ontario Court of Appeal was hearing the Stewart case, the Subcommittee on Com-

47. Copyright Act, CAN. REV. STAT. C-30 (1970).
51. Id. at 253 (1984).
52. Id. at 262 (1984).
puter Crime was concluding its deliberations on how the Canadian Criminal Code should be amended in order to encompass the problem of computer-related crime in Canada. The Subcommittee's Report recommended that the Criminal Code definition of property not be changed.

A 1986 decision of the Court of Appeal of Alberta in *R. v. Offley* reinforces the arguments against the reasoning in the *Stewart* case. The facts in *Offley* were similar to those in *Stewart*. The accused was a retired Royal Canadian Mounted Police staff sergeant who operated his own security company. His clients often called upon him to do security checks to determine if job applicants had criminal records.

To obtain information concerning the applicants, Offley requested name checks to be done for him by the Edmonton City Police Department through the Canadian Police Information Center (CPIC), a national law enforcement data base system. He was told that only law enforcement agencies were privy to such records and his request was refused.

He then approached a constable of the Edmonton City Police and offered to pay him $2.00 per name for each CPIC search. The constable reported the incident to his superior and a plan was devised to apprehend Offley. Upon receipt of money from the accused in exchange for the CPIC name checks, Offley was arrested, charged with and later convicted of theft of information, (property of the City of Edmonton Police Department) and with counseling with intent to procure or facilitate theft of information contrary to Section 109(b) of the Criminal Code.

---

55. 45 Alta. 2d 23 (1986).
56. Section 109 states as follows:

109. Every one who
(a) being a justice, police commissioner, peace officer, public officer, or officer of a juvenile court, or being employed in the administration of criminal law, corruptly
(i) accepts or obtains,
(ii) agrees to accept, or
(iii) attempts to obtain, for himself or any other person any money, valuable consideration, office, place or employment with intent
(iv) to interfere with the administration of justice,
(v) to procure or facilitate the commission of an offense, or
(vi) to protect from detection or punishment a person who has committed or who intends to commit an offense, or
(b) gives or offers, corruptly, to a person mentioned in paragraph (a) any money, valuable consideration, office, place or employment with
Belzil, J.A. on behalf of the majority stated that the issue on appeal was: "whether protected information is property capable of being stolen." After a full review and analysis of the reasoning in Stewart, Belzil concluded: "With all respect I do not agree with the majority decision of the Ontario Court of Appeal in Stewart."

In reviewing the wording under Section 283 relating to theft, Belzil found that:

What constitutes anything “animate or inanimate” in Section 283 must, in my view, be determined by the intrinsic nature of the “thing” and not by its quality. If information per se is intrinsically incapable of being an “inanimate thing” the qualifying of it as being “confidential” will not make it so...

Is the person who reveals a personal secret entrusted to him by a friend to be guilty of theft? Or the person who reads a confidential memo inadvertently left on his desk?

The decision of the Alberta Court of Appeal in Offley concluded that "confidential information is incapable of being stolen."

Offley’s appeal was allowed, the conviction of the trial court was quashed and a verdict of acquittal was entered.

The cases of Stewart and Offley now represent juxtaposed interpretations of the meaning of property under Section 283 of the Criminal Code. Whether confidential information will be deemed to be property for the purpose of that Section will be determined in Stewart’s appeal to the Supreme Court of Canada. It is argued that the decision in Stewart should be overturned in favor of a more restricted and traditional interpretation of the property definition as set out in the Offley case.

VI. “UNAUTHORIZED USE OF A COMPUTER SERVICE”-SECTION 301.2 OF THE CRIMINAL CODE

The previous cases illustrate the confusion associated with criminal prosecutions for computer based crimes. The 1985 amendments attempt to clarify the confusion and provide a standard set of rules for dealing with computer crimes.

1987] CANADIAN CRIMINAL CODE 179

---

57. 45 Alta. 2d 24 (1986).
58. Id. at 27.
59. Id.
60. 45 Alta. 2d 24, 29 (1986).
The new Section 301.2 of the Criminal Code appears to be in direct response to public protest and to the Supreme Court of Canada's requirement in *McLaughlin* for a specific statutory prohibition relating to the unauthorized access of computers.

The new subsection describing the offense of unauthorized use of computer services reads as follows:

301.2(1)

Every one who, fraudulently and without color of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under 387 in relation to data or a computer system is guilty of an indictable offense and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offense punishable on summary conviction.

(2) In this section, "computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; "computer service" includes data processing and the storage or retrieval of data; "computer system" means a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system; "electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing; "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system; "intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

1985, c.19 s.46.61

Certainly, had Section 301.2(1) been in place when *McLaughl*—

---

lin was charged, there is no doubt that the Supreme Court of Canada would have found him guilty of unauthorized use of a computer service.

VII. “Mischief”-Section 387(1.1) of the Criminal Code

A new offense for mischief in relation to data, Section 387(1.1), has also been added. This section eliminates a gap in the criminal law whereby law enforcement agencies were unable to prosecute computer “hackers”. The section reads as follows:

387(1.1) Every one commits mischief who wilfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with any person who is entitled to access thereto. \(^{62}\)

It should be noted that Section 387(1.1), as amended, falls under Part 9 of the Criminal Code ("Willful and Forbidden Acts in Respect of Certain Property"). \(^{63}\) Of special interest, is Section 385 in that Part which states: “Property means real or personal corpo-real property (1983-84, C.51, S.370).” On the other hand, Section 283(1) of the Criminal Code defines theft as an act of fraudulently and without colour of right, taking, or fraudulently and without color of right converting to one’s own use or to another’s use, “. . .anything whether animate or inanimate”. \(^{64}\) There is a clear difference then, between the definition of what can be stolen, that is, property, in Section 283(1) which falls under Part 7 of the Criminal Code and property as set out in Section 385 under Part 9 of the Criminal Code. In addition, the legislative draftsmen have specifically excluded data from being interpreted as “anything” under Section 283.

There is no new amendment to Section 283(1) incorporating the definition of data as set out in Section 301.2, which term is applicable in Section 387 under Bill C-18. The decision of the legislative draftsmen not to broaden the definition of property for the purposes of the theft provisions in the Criminal Code was based on the following reasoning:

For purposes of consistency in policy, misappropriation of information from a computer system should not be a criminal offense, if the same conduct in a non-computer environment is

---


\(^{63}\) Id. at § 387(1.1).

\(^{64}\) § 283(1) CAN. REV. STAT. Ch. C-34 (1970).
not criminally culpable. In this regard, it should be noted that Bill C-19 does 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 offenses of, dishonestly and without a claim 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. Addressing the problem in this manner avoids certain legal and socio-economic problems inherent in ascribing proprietary rights to information and thereby attempting to apply the existing theft and fraud provisions.65

VIII. THE COPYRIGHT ALTERNATIVE

In 1984, the White Paper on Copyright was published by the Department of Consumer and Corporate Affairs and the Department of Communications.66 In its analysis, the government recognized that criminal sanctions were required to deter some forms of copyright infringement. The White Paper proposed a section for criminal offenses and sanctions as follows:

*Criminal Offenses and Sanctions*

Given the economic nature of copyright, civil remedies will play the major role in copyright enforcement, for they are readily available in most instances.

There are some cases where criminal sanctions are the more appropriate instrument. Sometimes the magnitude of the infringement makes it either too costly or too complex for a private party to sue, or the socially reprehensible character of the conduct calls for public condemnation.

The current Act defines a number of separate and distinct offenses. Apart from the addition of specific technologies not explicitly covered by these provisions, such as film and broadcast performances, the existing offenses will be maintained.

However, the penalties will adequately reflect today's economic circumstances. The maximum penalty for these offenses will be a multiple of the value of the gross sales, the rental income or the remaining inventory of the infringing material, or a combination of these. The maximum fine for performances will be a multiple of the proceeds of any sale of tickets for the per-

65. Piragoff, supra note 28, at 311.
66. CANADA, CONSUMER AND CORPORATE AFFAIRS, FROM GUTENBERG TO TELIDON: A WHITE PAPER ON COPYRIGHT (Minister of Sup. and Serv. Can. 1984).
formance. If the values cannot be estimated, the maximum fine will be $25,000.

An indictable offense punishable by a fine, a jail sentence, or both, will be created to deal with serious commercial infringements that include the following ingredients:
— Deliberate perpetration;
— commission for commercial benefit or by way of trade;
— without color of right;
— either a potential or actual benefit to the perpetrator exceeding $5,000 or commission of the act knowing that it may prejudicially affect in a serious way any person’s copyright.

The fine will be established according to the rules mentioned above. The maximum penalty for such offenses will be from two to five years imprisonment in addition to or in lieu of the fine.67

The remedy provisions of the proposed amendments to the Copyright Act were designed to serve three main functions:

First, they provide restitution to copyright owners whose interests have been damaged by infringement. Second, injunctions and orders to deliver infringing goods or plates can be used to forestall potential infringements. Third, exemplary or punitive damages can be used to punish repeated or flagrant infringers and to serve as a warning to other would-be infringers.68

The White Paper on Copyright faced considerable criticism for certain of its recommendations, such as the proposal to limit the protection of copyright for computer software to five years. The Department of Consumer and Corporate Affairs has done a commendable job in responding to those criticisms and has recently published further revisions.69 Among other things, the new revisions provide for a term of protection for computer programs equal to the life of the author plus fifty years. Also, work created during the course of employment will be deemed to be owned by the corporate entity or person for whom the work was created. Corporate entities will be entitled to full rights of protection under the proposed Act.

A Federal-Provincial study on the Protection of Trade Secrets and Commercial Information was commenced in February, 1984. This study is examining the possibility of drafting Trade Secret leg-

67. Id. at 71.
68. White Paper, supra note 66, at 68.
69. CANADA, CONSUMER AND CORPORATE AFFAIRS, A CHARTER OF RIGHTS FOR CREATORS (Minister of Supply and Services Canada 1985) (report of the Subcommittee on the revision of Copyright by the Standing Committee on Communications and Culture).
islation which will afford protection for strategic business information.

It is argued by many that the Copyright Act and other intellectual property laws are more appropriate than the Criminal Code for dealing with offenses relating to misappropriation of proprietary information. Contrary to the *Stewart* court, it is this author's belief that in creating protection for confidential information, trade secrets, computer programs, or any other form of proprietary information, the Criminal Code should be the avenue of last resort.

IX. A COMPARISON OF RELEVANT CRIMINAL CODE AND CALIFORNIA PENAL CODE SECTIONS

Contrary to the federal system in Canada, in the United States, criminal sanctions for computer abuses are enacted on a state by state basis. California was one of the first states to enact such laws in large part due to the strong influence of the computer industry in the state. As a leading jurisdiction, California's Penal Code Sections will be compared with the corresponding Canadian provisions (see appendix).

California penalties for computer abuse are found in Section 502 of the Penal Code. Section 502(b) addresses the intentional access of computers, and Section 301.2 of the Canadian Criminal Code provides penalties for the unauthorized use of computers.

Section 502(b) is broader than Section 301.2. Section 301.2 only applies to the obtaining of computer services, the interception of any function of a computer system or the use of a computer with the intent to commit mischief. Conversely, Section 502(b) applies to accessing a computer for the purpose of fraud or extortion or for obtaining money, property or services.

Under the definitions clauses of the two sections it is noteworthy that Section 502 attempts to narrow the definition of computer system by excluding nonprogrammable pocket calculators. The Canadian definition has no such exclusions. It is unclear why pocket calculators in particular have been excluded under Section 502. Would not the same reasoning apply to microwave ovens or similar microchip devices? This is a further illustration of the definitional problems inherent in defining current technology. Section 301.2 allows for a defense relating to color of right where the accused can show that he had an honest belief that he was legally justified in doing the act.

The California Penal Code has specific sanctions for the theft
of information. Under the definition of property, such things as data, computer programs and other related documents have been incorporated. As previously discussed, Section 301.2 of the Canadian Criminal Code has no such provision.

An exception is made in Section 502(d) for employees accessing their employer's computers if such access was within the scope of employment. No such exception is made for Canadian employees under Section 301.2.

Section 502(c) of the California Penal Code parallels Canadian Criminal Code Section 387(1.1) relating to mischief. Section 502(d) addresses the malicious destruction or alteration of data. Under Section 387(1.1), the accused need only have acted wilfully whereas under Section 502(c), malicious intent is required. The objects of the criminal acts described in Section 502(c) are computer systems, computer networks, computer programs or data. The object of the offense set out under Section 387(1.1) is data. Reference to mischief against property is in Section 387(1) of the Criminal Code. "Data" is not property for the purposes of Section 387(1.1).

Sections 301.2 and 387(1.1) of the Canadian Criminal Code and Sections 502(e), (f), and (g) of the California Penal Code provide corresponding penalties upon conviction. Upon review of the two schemes for punishment, it is apparent that the Canadian sanctions are more severe. Even minor offenses under these sections bring with them penalties of least five hundred dollars or incarceration for six months or more. However, the California Penal Code punishments under Section 502 are more comprehensive. Violations are classified in accordance with the results of the criminal act as described and differentiated in Sections 502(f)(1), (2) and (3). California distinguishes between first offenses and second and subsequent offenses.

Section 502(g) provides for civil actions where a conviction is obtained. Under Canadian Criminal law, such a reference to civil actions is not within the jurisdictions of the federal government. Property and civil rights are under the sole responsibility of the provincial governments pursuant to Section 92(13) of the Constitution Act, 1982.

X. CONCLUSION

To date, the Canadian Courts have not been presented with a case involving charges under either Section 301.2 or Section

387(1.1). The definitions set out in Section 301.2(2) will undoubtedly be challenged by defense counsel as confusing, unworkable and inconsistent. Such definitions will become clarified as courts are called upon to decide which microchip devices should be included or excluded under such definitions in order to avoid absurd results such as prosecution for unauthorized use of a pocket calculator.

The Supreme Court of Canada will decide whether confidential information can be stolen when it hears the *Stewart* appeal. The Court will have to determine whether the decision of the Ontario High Court in *Stewart* which held that information is property under the Criminal Code should prevail or whether the *Offley* decision which rejected the reasoning in *Stewart* provides a more reasonable analysis of the intent of Section 283 relating to property. It is argued here that the *Offley* case should prevail.

It is clear that current Copyright Act penal sanctions are outdated. However, the Department of Consumer and Corporate Affairs and the Department of Communications are striving to create a revised Copyright Act which will adequately address infringements of computer software. The revised Copyright Act will include specific criminal code sanctions as outlined in the White Paper on Copyright.

Pursuant to the recommendation of the Subcommittee on Computer Crime, a Federal-Provincial study on the Protection of Trade Secrets and Commercial Information was commenced and will propose legislative protection for confidential information which in turn will reduce the need for criminal sanctions.

Comprehensive, technology-oriented statutes should be developed in Canada which will afford protection for intellectual property and which will include Criminal Code references for serious violations that go beyond a prescribed criminal threshold. Restricting the *Stewart* case will enhance the establishment of suitable definitional parameters for computer terms defined in the Criminal Code.

The Criminal Code differs from the California Penal Code in its conceptual approach to computer abuses. In Canada, the definition of property has remained narrow in its scope and only relates to anything whether animate or inanimate; it does not relate to information. In California, the Penal Code incorporates such concepts as trade secrets, data and computer programs into the definition of property. Furthermore, information is considered property and can be stolen in California. Attorneys representing
United States companies carrying on business in Canada, need to recognize these fundamental differences when attempting to protect the company's proprietary information and computer systems.
APPENDIX

CANADIAN CRIMINAL CODE AND CALIFORNIA PENAL CODE SECTIONS

CANADIAN CRIMINAL CODE

Unauthorized use of computer:

301.2(1) Everyone who, fraudulently and without color of right,
(a) obtains, directly or indirectly, any computer service,
(b) by means of an electromagnetic acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under Section 387 in relation to data or a computer system.

DEFINITIONS

301(2) In this section, "computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.
"computer system" includes data processing and the storage or retrieval of data; "computer system" means a device that, or a group of interconnected or related devices one or more of which,
(a) contains computer programs or other data, and
(b) pursuant to computer programs,
(i) performs logic and control, and
(ii) may perform any other function;
"data" means representations of information or of concepts that are being prepared or have been prepared in a computer system;
"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any functions 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;

CALIFORNIA PENAL CODE

Intentional access of computer:

502(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort, or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises, is guilty of a public offense.
502(d) Any person who intentionally and without authorization accesses any computer system, computer network, computer program, or data, with knowledge that the access was not authorized, shall be guilty of a public offense. This subdivision shall not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her employment.

DEFINITIONS

502(a) For purposes of this section:
(1) "Access" means to instruct, communicate with, store data in, or retrieve data from, a computer system or computer network.
(2) "Computer System" means a device or collection of devices, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that perform functions, including, but not limited to logic, arithmetic, data storage and retrieval, communication and control.
(3) "Computer network" means an interconnection of two or more computer systems.
(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.
(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.
(6) "Financial instrument" includes, but is
"functions" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;
"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

MISCHIEF:
387(1.1) Everyone commits mischief who wilfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

SANCTIONS:
301.2(1)(c) imprisonment for a term not exceeding ten years, or is guilty of an offense punishable on summary conviction. Summary convictions punishment is set out under Section 722(1) of the Criminal Code and refers to a fine of not more than five hundred dollars or to imprisonment for six months or more.
387(1.1) imprisonment for a term not exceeding ten years; or . . . punishable on summary conviction.

MALICIOUS DESTRUCTION OR ALTERATION OF DATA:
502(c) Any person who maliciously accesses, alters, deletes, damages, destroys or disrupts the operation of any computer system, computer network, computer program, or data is guilty of a public offense.

SANCTIONS:
502(c) Any person who violates any provision of subdivision (b) or (c) unless specified, is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.
(f)(1) A first violation of subdivision (d) which does not result in injury is an infraction punishable by a fine not exceeding two hundred fifty dollars ($250).
(2) A violation of subdivision (d) which results in an injury, or second or subsequent violation of subdivision (d) with no injury, is a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not
(3) As used in this subdivision, "injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was not altered, deleted, damaged, or destroyed by the access.

(g) In addition to any other civil remedy available, the owner or lessee of the computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Sections 1714.1 of the Civil Code.