HOUSE OF COMMONS
CANADA

REPORT OF THE SUB-COMMITTEE ON COMPUTER CRIME

STANDING COMMITTEE
ON
JUSTICE AND LEGAL AFFAIRS

June 1983

SUB-COMMITTEE

ON COMPUTER CRIME

CHAIRPERSON: Mme Céline Hervieux-Payette, Lib., (Montréal-Mercier, Qué.)
Mr. Ken Robinson, Lib., (Etobicoke-Lakeshore, Ont.)
Hon. Perrin Beatty, P.C., (Wellington-Dufferin-Simcoe, Ont.)

STAFF

Mrs. Monique Hébert, Research Branch, Library of Parliament

Pierre de Champlain

Clerk of the Sub-Committee

HOUSE OF COMMONS

Issue No. 18

Tuesday, June 14, 1983
Thursday, June 16, 1983
Tuesday, June 21, 1983

Chairman: Céline Hervieux-Payette

CHAMBRE DES COMMUNES

Fascicule nº 18

Le mardi 14 juin 1983
Le jeudi 16 juin 1983
Le mardi 21 juin 1983

Président: Céline Hervieux-Payette

Minutes of Proceedings and Evidence of the Sub-committee on

Computer Crime

of the Standing Committee on Justice and Legal Affairs

Procès-verbaux et témoignages du Sous-comité sur

Les infractions relatives aux ordinateurs

du Comité permanent de la justice et des questions juridiques

---

RESPECTING:

Order of Reference

CONCERNANT:

Ordre de renvoi

INCLUDING:

Final Report

Y COMPRIS:

Rapport final

First Session of the
Thirty-second Parliament, 1980-81-82-83

Première session de la
trente-deuxième législature, 1980-1981-1982-1983

Published under authority of the Speaker of the House of Commons by the Queen's Printer for Canada

Available from the Canadian Government Publishing Center, Supply and Services Canada, Ottawa, Canada K1A 0S9

Publié en conformité de l'autorité du Président de la Chambre des communes par l'Imprimeur de la Reine pour le Canada

En vente: Centre d'édition du gouvernement du Canada, Approvisionnements et Services Canada, Ottawa, Canada K1A 0S9

The Standing Committee on Justice and Legal Affairs has the honour to present its

NINTH REPORT

In accordance with its Order of Reference of Wednesday, February 9, 1983, your Committee assigned responsibility for the study of the subject-matter of Bill C-667, An Act to amend the Criminal Code and the Canada Evidence Act in respect of computer crime, to a Sub-committee.

The Sub-committee has submitted its final report to the Committee. Your Committee has adopted this report with amendments and asks that the Government consider the advisability of implementing the recommendations contained in the report.

The report of the Sub-committee, as amended, reads as follows:

TABLE OF CONTENTS

RECOMMENDATIONS

1. The Sub-committee recommends that the *Criminal Code* be amended to create two new offences: the unauthorized access (without colour of right) to a computer system, and the unauthorized alteration or destruction (without colour of right) of computerized data. The Sub-committee further recommends that Crown prosecutors be given the option of proceeding either by indictment or by way of summary conviction (para. 37).

2. The Sub-committee recommends that the definitions necessary to the description of the substantive offences be expressed, to the greatest extent possible in terms of function rather than of technology (para. 38).

3. The Sub-committee recommends that a comprehensive review of all matters relating to the effective detection and prosecution of computer crime be undertaken. Special attention should be paid to the adequacy of existing powers of search and seizure, the federal acts and treaties relating to international investigations and extraditions, and the wire-tap provisions of the *Criminal Code* as they relate to communications between computers (para. 47).

4. The Sub-committee recommends that every effort be made to ensure that law enforcement agents and prosecutors who are likely to deal with cases involving computer crime receive the necessary computer training to carry out effectively their functions (para. 48).

5. The Sub-committee recommends that the computer industry and institutional users recognize the potential for computer crime and adopt appropriate security measures (para. 51).

6. The Sub-committee recommends that the *Copyright Act* be amended to include computer software (para. 55).

7. The Sub-committee recommends that the federal government undertake a comprehensive study to examine the feasibility of extending patent and industrial design protection to computer programs (para. 56).

8. The Sub-committee recommends that both levels of government undertake a comprehensive joint study of trade secrecy law and adopt corrective measures (para. 58).

9. The Sub-committee recommends that the computer industry ensure, through self-regulation, a high standard of conduct in the industry (para. 65).

10. The Sub-committee recommends that knowledge of computer ethics be a qualification for educators involved in teaching computer skills and that the ethics of computer use be integrated into computer classes at all levels. (para. 67).

INTRODUCTION

1. The mandate of your Sub-committee is to examine the subject-matter of Bill C-667, an Act to amend the *Criminal Code* and the *Canada Evidence Act* in respect of computer crime.

2. Introduced for first reading by the Honourable Perrin Beatty on December 16, 1982, 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. A Sub-committee representing the three parties was established on March 10, 1983. The actual working group consisted of the Chairperson, Maître Céline Hervieux-Payette, Mr. Kenneth Robinson, Q.C., M.P., and the Honourable Perrin Beatty, M.P.

3. This arrangement, in the Sub-committee's view, worked out extremely well. Our limited membership and capacity to establish a non-partisan atmosphere in the course of our deliberations combined to make our work both effective and productive. For these reasons, we suggest that small sub-committees should be utilized more frequently to deal with the many issues which are of concern to Parliament.

4. In the course of our hearings, which began on March 17, 1983, the Sub-committee heard considerable evidence from a wide range of witnesses.(1) Appearing before us were individuals and groups with expertise in such diverse fields as computer technology, security and management, computer law, the law of intellectual property, law enforcement, banking, privacy rights and consumer protection.

5. The Sub-committee is deeply indebted to these persons who so generously gave of their time and expertise. The many different views expressed were extremely useful in providing us with a proper perspective on many of the issues at hand. We are especially grateful to the officials from the Department of Justice whose co-operation and assistance were unfailing, and to Ms. Susan Hubbell Nycum of the California law firm of Gaston, Snow and

Ely Bartlett, who was kind enough to share with us her knowledge of the American experience. The Sub-committee also wishes to acknowledge its gratitude for the assistance given in the course of the study and preparation of its report by the Clerk of the Sub-committee, Mr. Pierre de Champlain, and Mrs. Monique Hébert of the Research Branch of the Library of Parliament.

Céline Hervieux-Payette
Chairperson

A. The Computer Phenomenon

6. Since it was first introduced in 1946,(2) the computer has come to play such a dominant role in the processing of all kinds of information that it is difficult to imagine any large-scale enterprise able to function without it. According to industry sources, close to $40 million are transferred every day by electronic computer systems in Canada. In the United States, this figure is closer to $400 million. World-wide, it is $600 million.(3)

7. An indispensable tool to both business and government, the computer is now making inroads into the personal home market with typewriter size consoles that use the television screen for their video display. Anyone who has a bank account or engages in any kind of credit transaction routinely comes into contact with computers. As one witness appearing before the Sub-committee aptly put it:

> "Today I have come into contact with at least three computers since I left home in Toronto this morning. I flew to Montreal first thing this morning and Air Canada's computer gave me a boarding pass. I came on Via rail at lunchtime, and that gave me a ticket. Then I went to the Bank of Commerce, used my VISA card and drew out $100."(4)

The computer, in brief, is being integrated into every facet of human activity. It has the ability to collect, store, correlate, transfer and retrieve large amounts of data with relative ease and speed. While its present usefulness is undeniable, future technological advances will make it virtually indispensable.

8. However, there is an ominous side to be considered. Because of the computer's ability to process quantities of valuable information, it has become an obvious and attractive target of abuse. One hears of "system hackers" who, with some elementary knowledge of how computers function, gain access to telephone terminals and personal microcomputers. Contests are held in universities to see which student will be the first to break the computer's security—sometimes with the instructor's encouragement. Sophisticated fraud artists may steal thousands, and perhaps millions, of dollars from financial institutions by using the computer to reroute penny fractions into fictitious accounts. Disgruntled employees may place "time-bombs"* in the computer system, which are set to go off and destroy valuable programming once the employee has left the company.

9. Two well publicized "system hacking" incidents occurred in Canada. First, in the Dalton School case of 1980, a group of Grade Eight students from a private school in New York used the school's microcomputer to gain access to the data bases of a number of

* A "time-bomb" or "logic bomb" is a computer program inserted into a computer system, which damages the computer software or hardware, under predetermined circumstances. For example, a payroll system programmer could put a logic bomb in the computerized personnel system so that, if his name is ever removed from the personnel file, indicating termination of employment, a secretly coded program would be triggered resulting in the entire personnel files being erased.

Canadian companies and the federal government. Their method was not complicated. On the basis of published computer telephone numbers, the students were able to connect into the Canadian computers and, by simply trying out different passwords until one worked, succeeded in gaining access. Attempts were made on 21 Canadian computer systems. However, these attempts were not all successful. Some systems were well protected with sophisticated controls and codes. Only two firms indicated that their data banks had actually been penetrated and some information destroyed.

10. The second case occurred at the University of Alberta. In the summer of 1977, the University's computer was experiencing an unusually high degree of shutdowns, otherwise known as computer "crashes". Suspecting foul play, the University personnel, after close monitoring, apprehended a high school student who was in the process of using the computer system from one of the remote terminals located on campus. The student was not authorized to use the computer. He was charged with the offences of mischief, contrary to section 287(1)(c) of the *Criminal Code*(5) and the illegal use of a telecommunication facility, contrary to section 287(1)(b). Two other suspects also were charged with aiding and abetting in the commission of the offences, contrary to section 21(1) of the *Criminal Code*.

11. At trial, one accused was acquitted because of the lack of evidence. The second, the high school student caught red-handed, was found guilty on both counts. The third, the accused McLaughlin, was found guilty on the second count, but was acquitted on the mischief charge, since the evidence failed to establish his actual involvement in the computer "crashes".(6) McLaughlin appealed his sole conviction. On the ground that a computer system did not constitute a "telecommunication facility", the Alberta Court of Appeal, in a two-to-one decision, allowed the appeal and set aside the conviction, a ruling which was sustained in the Supreme Court of Canada.(7)

12. The *McLaughlin* case is important because it demonstrates that, for certain kinds of conduct which otherwise would be viewed as criminal, no criminal offence is committed since the provisions of the *Criminal Code* simply are inadequate. Since the relevant provisions of the *Criminal Code* were drafted at a time when computers did not exist, their formulation is not completely attuned to the new technology. Yet, with a rapidly advancing technology, the computer can be expected to play an ever-increasing role in our daily affairs. The need for legislative action to keep pace with this emergent technology and protect society from its ill-effects is apparent. Given the computer's capacity to process large amounts of valuable information, whether of a commercial or personal value, appropriate measures must be taken now before substantial economic or personal loss is sustained.

13. Witnesses appearing before the Sub-committee agreed that criminal sanctions were required to fill the void left by the McLaughlin case. However, there was little agreement on the form they should take. A number of witnesses argued that criminal sanctions should constitute but one of a variety of possible solutions, that emphasis should also be placed on improving the existing remedies or creating new ones. This view is shared by the members of the Sub-committee. In our opinion, it is important that all possible avenues of redress be examined and made available, where appropriate, so that the criminal law will be used only when necessary.

14. It may be useful at this juncture to mention that the term "computer crime", while a useful form of shorthand, is a misnomer. The more appropriate reference would be "com-

puter-related" or "computer-associated" activities. Moreover, since anti-social acts considered to be criminal in nature do not constitute a "crime" in Canada unless they are prohibited by law, it follows that the correct term which should be utilized is "computer-related" or "computer-associated misconduct". Indeed, the mandate of the Sub-committee is to propose amendments to the *Criminal Code* which would make a "crime" of those acts of "computer-related misconduct" not currently prohibited. Having raised this technical point, the remainder of this Report will refer to the term "computer crime" for the sake of convenience, whether the misconduct actually constitutes a crime or not.

B. The Incidence of Computer Crime

15. By all accounts, the incidence of computer crime is difficult to estimate. Some over-estimation may occur because any offence remotely associated with a computer is described as a computer crime. For instance, if a dishonest bank employee manually falsifies financial records which are subsequently fed unaltered into the bank's computer, no longer is this form of embezzlement called a fraud. Instead, a computer crime is committed, irrespective of the actual role played by the computer in the commission of the offence. Similarly, where a person is able to withdraw funds fraudulently from an automated banking device because he stole a credit card and obtained the password, again it is described as a computer crime, rather than the plain theft of a credit card. There is, in other words, a tendency to sensationalize what are otherwise fairly common offences.

16. Another reason why the incidence of computer crime is largely unknown is that the crimes may go undetected by the victim or, if detected, may go unreported, since victims, particularly those in the business community, may prefer not to attract any adverse publicity. Other reasons may be that the matter can be adequately dealt with internally, or the loss is too insignificant to warrant serious action.

17. There is very little empirical data which clearly demonstrate that computer crime poses a serious problem. According to a survey conducted by the Ontario Provincial Police between 1980 and 1981, of the 321 responses received from the 648 companies canvassed, only 13 reported experiencing a loss through computer crime, two-thirds of which involved theft of computer processing time and malicious damage to the computer files or equipment. Of these 13 incidents, only five were reported to the police at the time, and only three prosecutions appear to have been undertaken.(8)

18. Representatives from the Canadian Bankers' Association testified that, to their knowledge, members of the Association had never experienced a "pure" computer crime, one where the computer was instrumental in, rather than incidental to, the commission of an offence. Other evidence suggests that approximately 75 cases are reported annually worldwide, with a total annual loss of approximately $40 million.(9)

19. This evidence is in stark contrast to the often-heard "tip of the iceberg" theory which suggests that 85% of all computer crimes go unreported, with estimated annual losses in the billions of dollars. The evidence presented to the Sub-committee does not support this high estimate. Based on the testimony given, it is probably safer to conclude that the actual incidence of computer crime simply is not known. A comprehensive study has never been undertaken in Canada to estimate the occurrence rate and we do not feel that one is neces-

sary at this time. In our opinion, the fact that relatively little is known about the incidence and seriousness of computer crime is not a justification for legislative complacency. We must still have regard for the potential harm to society. Legislative action is needed to proscribe actual crimes and deter offenders.

C. The Criminal Law: The Existing Framework

20. One conceptual way of approaching computer crime is to distinguish between the computer as an instrument of crime, and the computer as the object of crime.

21. In the first category, the computer is used as a tool in the commission of the offence. The offence itself is not new. Only the means by which it is carried are new. The most important class of offences falling within this category are the computer-assisted frauds, that is, offences which have been successfully prosecuted under the existing provisions of the *Criminal Code*.

22. The second category, where the computer is the object of crime, is not so clear-cut. There are the "physical" offences, where there is tangible damage to, or the physical theft of, the computer or its components. Included in this category are the conventional theft and mischief offences. These offences also are successfully prosecuted under existing law.

23. The real problem arises when the computer, as the object of crime, sustains no tangible damage, as was the situation in the *McLaughlin* case. It will be remembered that McLaughlin was acquitted on the mischief charge because there was insufficient evidence linking him to the computer "crashes". Unless there is some kind of actual interference with the lawful use, enjoyment or operation of the computer, the mischief provisions of the *Criminal Code* will likely be inadequate.

24. An attempt recently was made to bring the activity within the general theft provisions of the *Criminal Code*. In the case of *R. v. Stewart*(10), the Crown alleged that the accused Stewart was guilty of counselling the theft of "information" belonging to the complainant hotel when the accused approached a hotel employee in order to obtain a copy of the computerized list of employees which contained their names, addresses and telephone numbers. This computer list, apparently, was to be used for the purpose of unionizing the hotel employees.

25. The trial judge dismissed the Crown's submissions, holding that the term "anything" whether tangible or intangible, used in the theft provisions of section 283 of the *Criminal Code* had to be capable of being property. Confidential information such as a list of employees was not property for the purpose of the law of theft. Anyone who takes or converts confidential information only, it was held, does not take or convert "anything" as that term is contemplated by section 283.

26. Since the Supreme Court of Canada effectively ruled out the possibility of equating computers with a telecommunication facility, a variety of activities violating the integrity of the computer system is not proscribed.

27. The nature of the activity involved in these abuses which are not prohibited under the *Criminal Code* covers a broad range. At one end of the spectrum is the so-called "joy-

riding" where essentially harmless "trespassers" seek the adventure and challenge of breaking into someone else's data base, without any intention of altering or destroying the data. At the other end of the spectrum is the more serious and sophisticated industrial espionage, where a competitor copies, without leaving any traces, computerized information which is both confidential and valuable, such as information on a large land development project or new oil discoveries. Even if the information has no economic value, the potential for injury may be great. For instance, a wrongdoer could gain access to computerized personnel files and use the information for a variety of improper actions.

28. Regardless of the severity of the abuse, the Sub-committee is of the view that criminal sanctions are necessary to curb this kind of conduct. This view was widely shared by all witnesses appearing before us. However, there was no clear consensus as to the exact nature such reform should take.

D. The Criminal Law: Proposed Amendments

29. Some witnesses argued that the definition of the term "property" should be extended to cover "information" or "computer-stored information" so that the existing provisions of the *Criminal Code* could apply. The Sub-committee questions this approach. In our view, it would be ill-advised to grant a proprietary interest in information per se, something which does not exist even in the civil law. 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.

30. Even with the statutory monopolies of copyright, patent, trademark and industrial designs, the creator, inventor or designer of the work is not given exclusive ownership rights in his creation, invention, or design. What is granted is more akin to an exploitation right, for a limited period of time. For example, the author of a book has, under the *Copyright Act*,(11) the sole right to "produce or reproduce" his book. Others are not precluded from drawing from the book. They simply may not make copies of it or copy its content, as that is the exclusive right of the author and his assignees, for the author's life plus 50 years. Similar, though not parallel, considerations come to bear with the remaining statutory monopolies. For these reasons, we believe that extending the definition of "property" to include "information" may lead to more problems than it would resolve.

31. A second reason to avoid this course of action is that it would confer on computer-stored information a status different to that of conventionally stored information. We are not persuaded that the medium of storage should govern the legal protection extended. Information taken from a filing cabinet or a computer is nevertheless stolen information. In our view, in order to be consistent, information must be given an even treatment, regardless of its storage medium.

32. Another possibility is the creation of an entirely separate statute specifically to deal with all matters relating to the computer. This possibility, which was not recommended by any witness appearing before us, is problematic for several reasons. Firstly, in order to introduce worthwhile legislation, far more time and study would be required in order to obtain a proper perspective. In our view, it is more important to introduce limited amend-

ments than to await the introduction of an all encompassing statute. Secondly, for the reasons stated above, it would be undesirable to treat computer crime differently than any other crime. If the conduct is criminal in nature, it properly belongs in the *Criminal Code*. Thirdly, it is unlikely that Parliament has the necessary legislative jurisdiction to enact such a law, given the potential for conflict with the provinces' legislative authority.

33. The prevalent view expressed by the witnesses appearing before us involves the creation of distinct provisions in the *Criminal Code* specifically to protect the integrity of computers. One of these would make the unauthorized access to a computer system a crime. In a draft proposal submitted to the Sub-committee, the Canadian Bar Association proposes that "everyone who, without lawful excuse, obtains the use of a computer system or any part thereof, without the consent of the owner" be made a criminal offence. Variants of this proposal which have been suggested, although not in legislative form, consist of making it an offence to interfere without lawful authorization with a computer, to use the computer in an unlawful manner, to take data without authority or to obtain computer services without authorization.

34. A number of witnesses recommended that a second offence should be enacted to proscribe the more reprehensible conduct of actually doing something to the data once access to the computer has been gained. In this regard, the Canadian Bar Association recommends the creation of an additional measure whereby an offence would be committed by "everyone who, without lawful excuse, alters or destroys computer programs or computer software without the consent of the owner." This approach, which deals with the alteration or destruction of data, is fairly representative of those who favour an additional offence.

35. The Sub-committee is in general agreement with this approach. However, an argument can be made that the second offence is already covered by the simpler "unauthorized access" offence, and that the seriousness of the abuse can adequately be addressed by making the offence a "dual procedure" offence and by providing for a broad range of sentences.

36. The Sub-committee does not support the latter view. In our opinion, the expediency factor must give way to the requirement that the criminal law be precise and fair. There is, in our view, a substantial difference between the two types of misconduct. They should not be dealt with on the strength of the same evidence.

37. The Sub-committee therefore recommends that the *Criminal Code* be amended to create two new offences: the unauthorized access (without colour of right) to a computer system, and the unauthorized alteration or destruction (without colour right) of computerized data. The Sub-committee further recommends that Crown prosecutors be given the option of proceeding either by indictment or by way of summary conviction.

38. The Sub-committee does not favour any specific wording of the proposed amendments. However, we have been repeatedly forewarned of the dangers of tying the definitions down to the current technology. Great improvements are being made in the area of computer technology. It is crucial that the definitions utilized avoid technical terms likely to be obsolete in the foreseeable future. It is therefore recommended that the definitions necessary to the description of the substantive offences be expressed, to the greatest extent possible, in terms of function rather than of technology.

39. As discussed earlier, the incidence of computer crime is largely unknown. In order to assess properly the dimensions of the problem, some contend that it would be desirable to enact compulsory reporting provisions. The Sub-committee does not favour this approach. Compulsory reporting provisions are not generally required under the *Criminal Code*, even with the most serious crimes such as homicide. To require that computer crimes be reported when most other offences are not cannot be justified, in our view. Moreover, to enact such a provision would be ill- advised, given its largely unenforceable nature.

E. The Canada Evidence Act

40. Part of the Sub-committee's mandate was to examine possible amendments to the Canada Evidence Act. Section 6 of Bill C-667 proposed to amend the existing *Canada Evidence Act* by providing that computer printouts be treated as original documents for the purpose of their admissibility into evidence.

41. This above amendment appears to have been proposed in response to the 1979 case of *R. v. McMullen.*(12) In this case, the court held that, in order to admit computer printouts into evidence, the nature and kind of evidence required would have to reflect the facts of the complete record-keeping process which, in the case of computer printouts, included the procedures and processes relating to the input of entries, storage of information, and its retrieval and presentation. If such evidence was beyond the ken of the manager, accountant or the officer responsible for the records, it was stated that the printout would not be admissible.

42. This ruling was not well received, particularly by the representatives of financial institutions. They objected both because it contemplated the introduction of evidence which might expose their computer security—since the computer processes and procedures had to be proven—and because it might require the testimony of too many bank employees who would need time off from work in order to give their evidence in court.

43. The *McMullen* case appears to have been largely superseded by the more recent case of R. v. Bell and Bruce.(13) The latter case decided that computer printouts constituted "records" within the meaning of section 29(2) of the *Canada Evidence Act*, since they were the only source of reference available to the bank as to the state of its bank accounts. As a "record" coming within the meaning of s. 29(2), the computer printout would be admissible on the strength of affidavit evidence.

44. Since the decision in *Bell and Bruce*, the alleged difficulties raised in the *McMullen* case appear to have resolved themselves in practice, although there is still much debate in academic circles as to the actual extent to which *Bell and Bruce* overrules the *McMullen* case.

45. The Sub-committee has received little evidence on this aspect of its mandate. On November 18, 1982, the government introduced Bill S-33, an Act to give effect, for Canada, to the Uniform Evidence Act adopted by the Uniform Law Conference of Canada. Bill S-33, which *inter alia* deals with the admissibility of computer printouts, is before the Senate Standing Committee on Legal and Constitutional Affairs. It is therefore not our intention to

make specific recommendations: the Sub-committee is satisfied that the provisions of the Bill are receiving every consideration. However, we affirm the importance of the work before the Senate Committee.

F. The Problems of Law Enforcement

46. By their nature, computer crimes are not easily detectable. Evidence presented to the Sub-committee suggests that, with some computer crimes, discovery is frequently no more than a matter of chance. The Sub-committee appreciates the complexities associated in effectively detecting and successfully prosecuting computer crimes, particularly those involving transborder data flows. Because of this fact, there is a real need further to develop the procedures available to detect and to gather the necessary evidence.

47. The Sub-committee therefore recommends that a comprehensive review of all matters relating to the effective detection and prosecution of computer crime be undertaken. Special attention should be paid to the adequacy of existing powers of search and seizure, the federal acts and treaties relating to international investigations and extraditions, and the wire-tap provisions of the *Criminal Code* as they relate to communications between computers.

48. To state that the techniques and powers of law enforcement must be adequate to deal effectively with computer abuses is addressing but one dimension of the problem. Another dimension rests with the need to ensure that the personnel assigned to detect and prosecute computer crimes obtain the necessary computer expertise. Computers are complex systems which can easily overwhelm those who have little or no knowledge of the field. The Sub-committee therefore recommends that every effort be made to ensure that law enforcement agents and Crown prosecutors who are likely to deal with cases involving computer crime receive the necessary computer training to carry out their functions effectively.

G. Additional Measures

1. Security Standards

49. As stated earlier, the Sub-committee firmly believes that the criminal law should constitute only one of the possible solutions to computer crime. Of all the other measures which were presented, the most important, in our view, are those which involve security measures.

50. Evidence presented at the hearings suggests that many computer crimes could have been averted if proper security measures had been implemented. The need for self-regulation within the industry is apparent. In our view, all computer systems which store valuable information, whether of commercial or personal value, must at least meet adequate security standards.

51. The Sub-committee does not recommend compulsory security standards, although they have been suggested by a few witnesses. It may well be that, at some future date, there

will be a need to enact appropriate regulations. In the interim, we recommend that the computer industry and institutional users recognize the potential for computer crime and adopt appropriate security measures.

2. Civil Remedies

52. Civil remedies are an important complement to the criminal law. In many instances, the victim of a computer crime may not want to press charges against the perpetrator, preferring to bring a civil action in order to get compensation for the loss sustained. For instance, if a video game pirate steals a program and then proceeds to sell pirated copies of the game, the program's creator may prefer to recoup his or her losses rather than send the offender to prison. Knowing that the offender is incarcerated may be of little consolation to a victim who, because of the piracy, is on the verge of bankruptcy.

53. The civil remedies which fall under federal jurisdiction are the statutory monopolies of copyright, patent, industrial design and trademarks. Of these, copyright and patent law appear to offer the best hope of providing some form of relief to the victim where the object of crime is the computer software. However, the weight of opinion seems to favour copyright protection.

54. Under the current *Copyright Act*, computer software is not specifically included in the protected works under the Act. In practice, many creators claim copyright for their programs, but the law itself is uncertain. We have heard evidence from a number of copyright experts who are convinced that copyright protection is the most appropriate vehicle. In 1978, the United States amended its copyright laws to include computer software, following a thorough study by a presidential committee on new technological uses.

55. The Sub-committee notes that a revision to the Canadian *Copyright Act* is in the final stages of preparation. Consistent with our view that the victims of computer crime should have as many avenues of redress as possible, we believe that copyright protection should be extended to computer software products. We therefore recommend that the *Copyright Act* should be amended to include computer software.

56. It may be that patents and industrial designs offer possibilities for the protection of computer programming. Because the Sub-committee received little testimony of this issue, we refrain from making a judgement. We recommend, however, that the federal government undertake a comprehensive study to examine the feasibility of extending patent and industrial designs protection to computer programs.

57. As with the federal statutory monopolies, the law of trade secrecy is underdeveloped. At present, trade secrets protection, which exists only at common law, works fairly well when there is a clear confidential relationship between two parties as, for example, in the case of an employee who is bound to respect the confidential information received in the course of his employment. The protection becomes more doubtful when the trade secret is conveyed to third parties who are not themselves privy to the original agreement of confidentiality.

58. The Sub-committee believes that the law of trade secrecy could be vastly improved to offer more protection to all victims whose trade secrets have been breached, either because of a computer crime or in other ways. Losses resulting from the theft of trade secrets can be

extensive. At present, trade secrecy is a matter falling within provincial jurisdiction and no province has enacted trade secrecy legislation. In the future, a need to criminalize the theft of trade secrets may arise. The Sub-committee, however, recommends that both levels of government undertake a comprehensive joint study of trade secrecy law and adopt corrective measures.

59. Given the computer's incredible capacity to collect and process data, many are deeply concerned about its potential threat to the confidentiality of personal information. Privacy rights advocates even have recommended that the custodians of personal information should be held criminally liable for unlawful access to the information due to inadequate security. While sympathetic to their concerns, the Sub-committee cannot support such drastic measures at this time. However, steps should be taken to ensure that personal information, whether stored in a computer or elsewhere, is adequately protected from those who have no right to have access to it.

60. Privacy rights are largely a matter of provincial jurisdiction, but no province has taken the initiative to enact comprehensive measures to deal with the protection of all personal information. The province of Quebec may be cited for its innovative law on access to public documents and the protection of personal information.(14)

61. The basic framework of the Quebec law is that information publicly held is to be treated confidentially unless the person the information concerns authorizes its disclosure. Moreover, the government can issue regulations fixing the appropriate security standards to ensure the information's confidentiality. Finally, penal sanctions are provided for any unlawful disclosure of publicly held personal information.

62. While there are a number of measures which exist under other federal and provincial statutes which provide for the confidential handling of personal information, for example, sections 62 and 63 of the federal *Privacy Act* and section 241 of the *Income Tax Act*,(15) no truly comprehensive privacy statute has been enacted. This underdeveloped area of the law, in our view, should be subject to further study.

3. Code of Ethics/Code of Conduct

63. Since the computer industry is relatively new, few measures govern the activities of those who work with computers. Although the information contained in the computer may be highly valuable or sensitive, there are no compulsory codes of professional conduct which must be adhered to, as is required for other disciplines, such as law and medicine. The Canadian Association of Data Processing Service Organizations (CADAPSO) has developed a code of conduct which has provisions dealing with standards of conduct affecting the public interest, and relations with members and non-members engaged in the provision of data processing services.(16) However, membership in CADAPSO is not mandatory.

64. The Canadian Information Processing Society (CIPS) is in the process of developing a certification accreditation process for systems programmers so that the industry can regulate itself. At this time, the process is nowhere near completion.(17)

65. The Sub-committee supports these efforts which may deter would-be computer criminals and ensure a high standard of moral behaviour among computer users. If self-regulation fails, compulsory accreditation or licensing may have to be considered, but the current

situation does not justify such action. The Sub-Committee therefore recommends that the computer industry ensure, through self-regulation, a high standard of conduct in the industry.

66. There is growing evidence that users of computer systems are not, in all cases, aware of their ethical responsibilities. Adolescents and young students are of special concern because their level of maturity can be far less developed than their computer skills.

67. The Sub-committee believes that much could be gained if proper ethical conduct were made an integral part of computer training. If appropriate ethical values are instilled in the individual at an early date, they may serve to decrease the potential for computer crime. The Sub-committee therefore recommends that knowledge of computer ethics be a qualification for educators involved in teaching computer skills and that the ethics of computer use be integrated into computer classes at all levels.

CONCLUSION

68. Early in its deliberations, the Sub-committee became aware that it was impossible to separate the issue of computer crime from the much broader issue of "information". Because of this observation, we have made recommendations in areas which may well go beyond our narrower mandate of computer crime and the criminal law. Nevertheless, we believe that it is desirable to have all possible remedies in place. Amendments to the *Criminal Code* constitute only one of these. In terms of deterrence, the fact that a computer criminal may be liable for damages for the loss occasioned by his or her misdeed can be as effective a deterrent as the imposition of a fine or a term of incarceration.

69. Improved remedies are therefore necessary to provide the victim of a computer crime with the most suitable form of redress. These measures, however, arise only after the crime has been committed. In our view, it is of greater importance to ensure that all possible preventive measures are vigourously pursued. If computer systems are adequately secured, and those most likely to use them are properly educated, a number of wrongful acts which otherwise might occur will be averted.

REQUEST PURSUANT TO STANDING ORDER 69(13) OF THE HOUSE OF COMMONS

70. Pursuant to Standing Order 69(13) of the *Permanent and Provisional Standing Orders of the House of Commons*, the Committee on Justice and Legal Affairs requests that the Government table a comprehensive response within 120 days of the presentation of this Report to the House of Commons.

NOTES

(1) For the list of witnesses appearing before the Sub-committee, see Appendix "A"

(2) The first computer came into existence in 1946 at the University of Pennsylvania. It was called the "Electronic Numerical Inegrator and Calculator" (ENIAC). For greater detail, see S. Sokolik, "The Computer Crime—The Need for Deterrent Legislation" *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, pp. 353-385, at p. 354.

(3) *Security World*, January 1982, p. 28.

(4) Evidence given by Mr. Peter Ward of Peat, Marwick and Partners. *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, April 27, 1983, 4:18.

(5) R.S.C. 1970, c. C-34.

(6) *R. v. Christensen et al.* (1978), 26 *Chitty's Law Journal*, p. 348 (Supreme Court of Alberta, Trial Division).

(7) *McLaughlin v. R.* (1979), 12 C.R. (3d) 391 (Alberta Court of Appeal); and *Her Majesty the Queen v. McLaughlin* (1980) 2 S.C.R. 331 (Supreme Court of Canada).

(8) Entitled the "Ontario Provincial Police, Computer Crime and Security Survey", this survey was produced by Superintendent G.W. Allen, of the Commercial Crimes Branch of the R.C.M.P., who appeared before the Sub-committee on March 17, 1983.

(9) Evidence given by Mr. Peter Ward of Peat, Marwick and Partners. *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, April 27, 1983, 4:6.

(10) *R. v. Stewart* (1982), 68 C.C.C. (2d) 305.

(11) R.S.C. 1970, c. C-30.

(12) *R. v. McMullen* (1979), 100 D.L.R. (3d) 671.

(13) *R. v. Bell and Bruce* (1982), 65 C.C.C. (2d) 377.

(14) *An Act respecting Access to documents held by public bodies and the Protection of personal information*, S.Q. 1982, c. 30.

(15) Respectively, S.C. 1982, c. 111; and R.S.C. 1970, c. I-5, as amended.

(16) For greater detail, see *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, May 19, 1983, 10:7.

(17) *Minutes of Proceedings and Evidence* of the House of Commons Sub-committee on Computer Crime, May 25, 1983, 12:11.

Appendix "A"

WITNESSES WHO APPEARED BEFORE THE SUB-COMMITTEE

	Date of Appearance
Department of Justice	
Mr. Norman Hill, Project Chief, Theft and Fraud Project	March 17, 1983
Mr. Neville Avison, Chief, Research and Statistics	March 17, 1983
Royal Canadian Mounted Police	
Superintendent George W. Allen, Commercial Crimes Branch	March 17, 1983
Cerberus Computer Services Inc.	
Mr. James Finch, Toronto	March 23, 1983
Mr. Collin C. Rous, Toronto	March 23, 1983
Canadian Business Equipment Manufacturers Association	
Mr. John Reid, Chairman of the Legislation Committee (CBEMA)	April 19, 1983
Mr. Howard Kaufman, Vice-President of Xerox	April 19, 1983
Mr. John Dean, Senior Legal Advisor of IBM	April 19, 1983
Peat, Marwick and Partners	
Mr. Peter Ward, Toronto	April 27, 1983
University of Western Ontario	
Professor John Palmer, London, Ontario	May 3, 1983
Professor David H. Flaherty, London, Ontario	May 3, 1983
Landspan International of Canada Ltd.	
Mr. Peter J. Lawrence, President/Director	May 10, 1983
Mr. J. Ian Henderson, Vice-President and General Counsel Ottawa, Ontario	May 10, 1983
Mr. Morvin Gentleman, National Research Council	May 11, 1983
Mr. Frank Spitzer, Consultant, Toronto	May 11, 1983
Mr. Dave Conway, Manager, Resources Protection, Mitel Corporation, Kanata, Ontario	May 17, 1983
Professor Tony J. Juliani, Department of Criminology, Ottawa University	May 17, 1983
Professor Grant Hammond, Counsel, Law Center, University of Alberta, Edmonton, Alberta	May 18, 1983
Mr. George E. Fisk, Barrister and Solicitor, Gowling and Henderson, Barristers, Ottawa, Ontario	May 18, 1983
Mr. Paul C. Boire Sr., President, Canadian Association of Data Processing Service Organizations (CADAPSO), Ottawa	May 19, 1983
Mr. D.W. Kay, District Manager, Datacrown Inc., Ottawa	May 19, 1983

Department of Consumer and Corporate Affairs	
Mr. Tony Butler, Senior Policy Advisor	May 24, 1983
Mr. Bruce Cauchman, Policy Advisor	May 24, 1983
Canadian Information Processing Society, Toronto	
Mrs. Sally Woodhead, Chairman, Special Interest Group on Computer Security	May 25, 1983
Canadian Bankers' Association	
Mr. R.M. MacIntosh, President	May 26, 1983
Mr. E. Jestin, Supervisor, Internal Control, Evaluation, The Bank of Nova Scotia	May 26, 1983
Ms. Pat Learmonth, Co-ordinator of Communications	May 26, 1983
Consumers' Association of Canada	
Ms. Christine Bisanz, Acting Director of Association and Activities	May 31, 1983
Ms. Christine Elliott, Member, Ontario Branch	May 31, 1983
Gaston, Snow and Ely Bartlett, Palo Alto, California	
Mrs. Susan H. Nycum, Attorney-at-Law	June 1, 1983
Canadian Bar Association	
Mr. Yves Fortier, President	June 8, 1983
Mr. Bernard E. Blanchard, Executive Director	June 8, 1983
Ms. Judith Kingston, and	June 8, 1983
Mr. Charles W. MacIntosh, Q.C., of the Standing Committee on Law, Science and Technology	June 8, 1983
Mr. Stephen Georgas, Barrister and Solicitor, Toronto	June 9, 1983
Department of Justice	
Mr. E.A. Tollefson, Co-ordinator, Criminal Code Review	June 9, 1983
Mr. Norman Hill, Project Chief, Theft and Fraud Project	June 9, 1983

Appendix "B"

SELECTED BIBLIOGRAPHY

The "Selected Bibliography" lists the most important published works that were consulted in the study and preparation of this Report. A more comprehensive list of titles, containing over 300 magazine and scholarly articles, was compiled by the Library of Parliament. This list may be obtained by contacting the Clerk of the House Sub-committee on Computer Crime.

Becker, J., "Rifkin, A Documentary History", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 471-720.

Becker, J., "The Trial of a Computer Crime", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 441-456.

Hammond, G. R., "Quantum Physics, Econometric Models and Property Rights to Information", *McGill Law Journal*, Vol. 27, 1981, 47-72.

Ingraham, D., "On Charging Computer Crime", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 429-439.

Kling, R., "Computer Abuse and Computer Crime as Organization Activities", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 403-427.

Krieger, M., "Current and Proposed Computer Crime Legislation", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 721-771.

Palmer, J. and Resendes, R., Copyright and the Computer, Ministry of Supply and Services Canada, 1982.

Parker, D.B., "Computer Abuse Research Update", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 329-352.

Schjolberg, S., "Computer/Assisted Crime in Scandinavia", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 457-469.

Simkin, M., "Is Computer Crime Important", *Journal of Systems Management*, May 1982, 34-38.

Sokolik, S.L., "Computer Crime - The Need for Deterrent Legislation", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 353-383.

Taber, J.K., "A Survey of Computer Crime Studies, *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 275-327.

United States, Department of Justice, Bureau of Justice Statistics, Criminal Justice Resource Manual. Computer Crime, Washington, 1979.

Volgyes, M., "The Investigation, Prosecution and Prevention of Computer Crime: A State-of-the-Art Review", *Computer/Law Journal*, Vol. II, No. 2, Spring 1980, 385-402.

Watkins, P., "Computer Crime: Separating the Myth From the Reality", *CA* Magazine, Jan. 1981.

Whiteside, T., "The Annals of Crime", *New Yorker*, Aug. 22, 1977, (Pt 1); Aug. 29, 1977 (Pt 2).

A copy of the relevant Minutes of Proceedings and Evidence of the Sub-committee on Computer Crime (Issues Nos. 1 to 17 inclusive and 18 which includes this report) and a copy of the relevant Minutes of Proceedings and Evidence of the Standing Committee on Justice and Legal Affairs (Issues Nos. 117, 119, 131 and 132) are tabled.

Respectfully submitted,

CLAUDE-ANDRÉ LACHANCE,
Chairman.

MINUTES OF PROCEEDINGS

TUESDAY, JUNE 14, 1983

(20)

[*Text*]

The Sub-committee on computer crime met *in camera* this day at 3:40 o'clock p.m., the acting Chairman, Mr. Ken Robinson (*Etobicoke—Lakeshore*), presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternate Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee proceeded to the consideration of the draft report on computer crime.

At 5:30 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

THURSDAY, JUNE 16, 1983

(21)

The Sub-committee on computer crime met *in camera* this day at 5:05 o'clock p.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee resumed consideration of the draft report on computer crime.

At 6:14 o'clock p.m. the Sub-committee adjourned to the call of the Chair.

TUESDAY, JUNE 21, 1983

(22)

The Sub-committee on computer crime met *in camera* this day at 10.01 o'clock a.m., the Chairman, Mrs. Céline Hervieux-Payette, presiding.

Member of the Sub-committee present: Mrs. Hervieux-Payette.

Designated Alternates Members present: Messrs. Beatty and Robinson (*Etobicoke—Lakeshore*).

In Attendance: Mrs. M. Hébert, Researcher, Research Branch, Library of Parliament.

The Sub-committee resumed consideration of its Order of Reference dated Tuesday, March 1st, 1983. (*See Minutes of Proceedings, Tuesday, March 15, 1983, Issue No. 1*).

The Sub-committee resumed consideration of the draft report on computer crime.

On motion of Mr. Robinson (*Etobicoke—Lakeshore*), the Third Report of the Sub-committee on computer crime as amended was concurred in.

Ordered,—That the Chairman report the Report to the Standing Committee on Justice and Legal Affairs.

It was agreed,—That the report be printed within turnover format and green special cover.

On motion of Mr. Beatty, it was ordered,—That an additional 2000 copies be printed of Issue No. 18 of the Sub-committee's Minutes of Proceedings and Evidence.

At 12:00 o'clock p.m., the Sub-committee adjourned to the call of the Chair.

Pierre de Champlain
Clerk of the Sub-committee