present in the gallery. Professor Manning had warned that the Government's safeguards on the networking of computers are so lax that massive invasions of personal privacy would become possible. Perhaps if the Government had taken action then, when the problem of computer theft and unauthorized access became apparent, situations like the Dalton School mystery could have been avoided.

What is most striking about the Dalton School incident is that a group of Grade eight students, operating with a small micro computer in New York City, was able to use the telephone system to break into data banks here in Canada. When this sort of incident occurs, a great deal of discussion takes place about the fact that these children must be computer geniuses. They are not. They were run of the mill students who had no particular expertise that other students did not have. Most important, they were grade eight students.

If data bases here in Canada are vulnerable to that sort of intrusion from grade eight students, then it is time for us to recognize that we have a very serious problem and the Government must act on it.

I want to elaborate briefly on the areas where I believe current federal legislation fails to protect individuals and organizations from computer abuse. Here the distinction between computers as the object of abuse and computers as an instrument of abuse becomes useful. Where the computer is used as the instrument of crime, there have been successful prosecutions under various provisions of the Criminal Code. As it stands today, it is against the law to commit fraud, to transfer money from someone else's bank account to your own. That can be prosecuted under the Criminal Code as it exists today. There have been a number of instances such as that where prosecutions have been successful. There is concern over how the law applies in the present situation when it comes to the introduction of evidence into the courts and whether it is possible to prove that an offence had taken place and that the individual who was accused was the perpetrator of the offence.

I will say again that there is agreement that the law as it stands today for dealing with fraud or with the computer as an instrument of abuse is generally adequate, with the exemption of law relating to evidence as it stands today. It appears there is serious doubt as to whether it is possible to introduce the sort of evidence that is necessary to prove the crime. Unfortunately, the proof for some instrumentality cases is difficult to obtain. Since the Ontario Court of Appeal held in *Regina v. McMullen* in 1979 that computer print-outs were only admissible as evidence if they could be proven to be true copies of the original record, a heavy burden has been placed on the prosecution.

In 1981, the evidence task force, established by the federal Justice Department, proposed changes to the Canada Evidence Act which would require a person attempting to enter a document as evidence to prove, first, that the data upon which the print-out is based are of a type regularly supplied to the computer in the regular activities of the business; second, that the entries upon which the print-out is based were made in the regular course of business; and finally, that the computer program used in producing the print-out reliably and accurately processes the data in the data base.

One problem with this approach is that a computer print-out would still be treated differently from an ordinary manual record, in spite of the fact that these print-outs are not copies of business records but are the original business documents. Often, no other records except the original computer print-out are kept.

Since it appears that existing legislation is sufficient to charge criminals who use a computer as an instrument of a crime, an amendment to the Canada Evidence Act such as the one I have introduced could close any remaining loophole that might allow perpetrators of crimes of this variety to get off. In effect, the amendment would allow computer print-outs to be treated in evidence as originals.

Where the computer is the object of abuse, more serious problems arise because some forms of conduct—like the theft of ideas, software, or computer time—are simply not dealt with in the Criminal Code. These intangibles are not normally considered property in the legal sense. Other crimes like vandalism of hardware or the stealing of computer chips can clearly be prosecuted as criminal offences since something tangible is involved.

Consider the case where a firm has spent millions of dollars on research and development of a new high-tech item. Suppose someone without authority gains access to the computer system and obtains this valuable data. The thief may copy the information or he might steal it outright, leaving no information at all. As things stand now, it would be extremely difficult to prosecute him. Depending upon how the thief obtained the access code and entered the room containing the computer terminal, he might be convicted on a lesser offence, but he is unlikely to be convicted of theft of information.

Last summer, an individual went to court on charges of counselling an employee of a hotel to commit theft, fraud and mischief. The Crown alleged that he had approached the employee last year and offered him money in return for the names, addresses and telephone numbers of the hotel employees in connection with a union organizing drive. The information was contained on a computer print-out to which only senior executives of the hotel had access. In the fall, Mr. Justice Krever concluded that "confidential information is not property for the purpose of the law of theft in Canada". Consequently, currently under our Criminal Code, deprivation must occur in order for a theft to have been committed. Judge Krever stated that, while he had no trouble attributing a notional value to the confidential information, there was no suggestion in this case that the hotel would have ever sold the information. Therefore, they had not been deprived of anything. The accused was found not guilty on all charges.

• (1730)

Another situation for which there is no clear-cut legal sanction is the unauthorized acquisition of computer software. Again, because a program is really nothing more than a set of coded instructions that, when introduced to a computer,