with Members of Parliament, that knowledge of the issues is not very deep, that an understanding of the implications of the direction in which we are moving often is not very great. The Government's ability to make up its own mind as to the direction in which we should be going to ensure the maximum benefits from new technology and in order to ensure that we do not run into problems as new technologies develop is very much handicapped at the present time.

What we find is that in instance after instance the Government defers taking decisions and leaves Canadians in a position where they are unprotected and where the law is simply not adequate to deal with advances in new technology. What we find is that Government is not good at anticipating new problems coming along and putting legislation in place in a moment of calm when people are able to debate dispassionately a situation that may occur in the future. What generally happens is that after a crisis occurs or after there is an emergency which generates a good deal of public attention we find that the Government overreacts and brings in legislation that is far too sweeping and Draconian as a result of the temporary conditions created.

The recent fiasco over Crown Trust is a case in point. It took a threat to the security of the holdings of people who have investments in Canadian trust companies as well as considerable public concern before the Government was prepared to make amendments to improve the security for those people with investments in those companies. If we had recognized the potential problems that would exist, we would have served Canadians much better.

• (1720)

Nowhere is this problem more acute than in the field of computer crime. We have a situation where the law as it stands in Canada today is simply inadequate, as it is in the United States. Technology has simply rendered the Criminal Code irrelevant. Cases have already been demonstrated in the courts that the law as it stands today is simply not up to scratch with modern technology.

It is essential that Parliament act before it is too late, and there are more serious incidents which could jeopardize the security of Canadians in terms of personal privacy or which could result in the loss of proprietary rights of individuals which could cost literally millions of dollars to Canadian businesses and individuals. That is why I think it is essential for us to act today and do so in a moment of calm and with deliberation. I think it is essential that the Government itself be prepared to allow the Bill to go to second reading, to let it go to committee, to let witnesses who are expert in this field and are concerned with the whole field of computer crime be called. Let Parliament itself hold these hearings so that a consensus can be developed within Parliament and within the community that deals with computers as to what the best course of action is to take. The Government can then introduce its own legislation consistent with the recommendations of Parliament, and let us pass it speedily. The stalling must stop. The indecision must stop. The onus is on Parliament to act today.

To put things in some perspective, some experts have estimated that losses due to computer crime are as high as $20 million a year in Canada and $5 billion in the United States. In 1981, it was estimated that approximately one out of every ten EBP installations was subjected to computer crime.

An example of the vulnerability of computer systems is the Data Encryption Standard which is used to code and scramble confidential data in the United States. The DES is the only technique that has the approval of the National Security Agency, and yet, ever since its development in the early 1970s, experts have been arguing that its codes can be broken by anyone familiar enough with computers who was willing to take the time to devise the right program. To put the complexity of this program into perspective, let us describe it. The DES program involves scrambling all the pulses of a digital electronic message 16 times, transcribing this to the receiver, who must reverse the 16 scrambles. This is the type of sophisticated coding that experts say can be broken.

For Canadian businesses and Government, the computer has come to play a central role, and within the years to come its predominance will only increase. An ever increasing number of employees will have access to computer terminals accompanied by a growing understanding of their complexities. With the world of teleshopping, telebanking, and so on, advancing closer to our living rooms, and with the use of personal computers dramatically on the rise, even the strongest critics of computer crime legislation must agree that the computer will democratize white collar crime. Well within our lifetimes, school-age children will be capable of operating sophisticated computer programs and equipment. Electronic data processors will be no more novel to them than telephones and televisions are to us in the House of Commons today. Accompanying this familiarity and universality of computers will be a growing potential for computer abuse. That is why it is important that we act now to consider legislation to deal with this abuse.

A good illustration of this is the great Dalton School mystery where a number of Grade eight students from a New York private school attempted to tap into 21 Canada data systems, destroying files of at least two firms. Among the firms attacked, successfully or unsuccessfully, were Bell Canada, Canada Cement, Cable Share Inc., Honeywell, several universities and two federal Government data banks with dial-in access to the data banks. On May 9, 1980, as reported at page 888 of *Hansard*, I questioned the President of the Treasury Board (Mr. Johnston) about this matter. At that time, he stated his intention to:

—recommend to the Minister of Justice that amendments to the Criminal Code be considered for the purpose of making it clear that any such theft would be a crime under the Criminal Code.

Obviously some Members of the Government recognize the need to close the loopholes in criminal legislation so that there will be legal recourse against this type of crime. Unfortunately, they seem incapable of acting on their intentions.

On February 1, 1979, I asked another question of the President of the Treasury Board when Professor Eric Manning of the University of Waterloo, and an expert in this field, was