of which is the surreptitious interception of wire or oral communications, should be prohibited by the Criminal Law. Such devices, where found, must be subject to forfeiture to the Crown. It is recommended that no forfeiture action be commenced without the consent of the Attorney General. This would provide a means for protecting such legitimate use, as may be consistent with the policy of Parliament, in the fields of telecommunications, education, science, medicine or wherever else a bona fide employment exists for devices capable of the prohibited ends, but which are clearly not used therefor.

It is further recommended that in any prosecution under the above-described addition to the criminal law, or forfeiture action in relation thereto, the burden should be on the Crown to prove that the primary usefulness of any device in question is the surreptitious interception of wire or oral communications.

Industrial espionage is closely related to the subject of wiretapping and surreptitious electronic device surveillance, as well as to the general problem of protection of privacy. The prohibition of privacy-invading activity through the use of instruments for the interception of communications will itself strike at the common methods of industrial espionage. However, the Committee recommends that specific legislation be enacted by Parliament which provides the protection of the Criminal Law against activities which involve the procurement, use or disclosure of confidential business information with intent to commit industrial espionage. This would provide protection in an area which is presently unregulated by law, and which, where taken together with the proposed ban on wiretapping or use of electronic surveillance devices, and the Criminal Code provisions dealing with personation and bribery of an agent, should provide a reasonably comprehensive code of protection against industrial espionage.

Unauthorized abstraction of information from a computer or data bank is an activity which is closely analogous to theft of a telecommunication service. The recommendation that this be made a criminal offence is simply a statement that the law should keep pace with social and technological change. The present Criminal Code section seems to be premised upon the protection of the economic interest of the supplier of the telecommunication service. The proposed new section on computers and data banks would be premised upon the protection of the privacy, both commercial and personal, of the persons who are the subjects of the data stored or transmitted. This problem can be approached either by making the definitions of wiretapping and surreptitious electronic device surveillance wide enough to include the unauthorized abstraction of computerized data, or the activity can be specifically named in an amendment to the present section 273 of the Criminal Code.

PROVINCIAL RESPONSIBILITIES FOR THE PROTECTION OF PRIVACY

It should be pointed out that these prohibitions deal only with a few manifestations of a varied and complex nationwide problem, the optimum solution to which is not to be found within the Criminal Law, nor within any of the other enumerated powers constitutionally committed to the Federal Government. Control of wiretapping and surreptitious electronic device surveillance, whether by law-enforcement personnel, government agents or by private individuals is simply one aspect of the wider problem of protection of privacy. Both