Appendix F

Privacy and Data Protection Policy in Selected Foreign Countries[1]

Many Western European countries and Canada have also established policy to protect the collection and use of personal information. Many of these countries have created boards or commissions with responsibilities for overseeing government and private sector information practices, and acting as ombudsmen for individuals. Because the policies of these countries may serve as a model for policy actions in the United States, descriptions of the policies of several countries follow.

The Federal Republic of Germany

The Federal Data Protection Act became law on January 27, 1977. Its provisions apply to both computerized and manual personal information systems in both the public and private sectors. Registration of all private and computerized public information systems is required under the act. Although the general principles regarding rights of individuals and restrictions on the collection and use of personal information are the same for public and private organizations, the methods of regulating the two sectors differ.

The act provides for the appointment of a Federal Commissioner for Data Protection to supervise public sector information systems. This position was added to the draft legislation at the insistence of the West German legislature; the original government bill did not call for such an official. The Commissioner, who serves for a 5-year term and may be reappointed once, has the authority to investigate complaints, inspect information systems, require information from agencies, and make recommendations. The Commissioner does not have licensing power. Nor does the office have enforcement powers; rather, the head of each public agency is responsible for ensuring compliance by the agency. The Commissioner serves, therefore, in an advisory capacity rather than a regulatory one. Up to now, the advice of the Commissioner has been taken seriously by the Federal agencies, including the national security agencies and the Federal police. In essence, it has not been politically viable for the heads of Federal agencies to ignore the Commissioner's advice, which is nor-really given privately at first and later as part of a process of negotiation over competing interests in the use of information. The Federal Commissioner for Data Protection is subject to supervision by the government and reports to both the Minister of the Interior and to Parliament.

Private organizations maintaining personal information systems are supervised by the Land (State) authorities to which the organization belongs. For example, the Land authority that regulates banking activity is now responsible for ensuring that the banks also comply with data protection rules.

Sweden

Sweden was the first country to pass national legislation regarding the collection and use of personal information. The purpose of the 1973 Data Act was to protect the confidentiality of records, to rationalize the personal information policies of organizations, and to expand individual rights and state protection to private information systems. The Data Act covers all computerized personal information systems in the public and private sectors. It established a regulatory agency, the Data Inspection Board (DIB), which is independent of the government and has the responsibility for licensing all automated personal information systems in both the public and private sectors. The 1973 statute mandated DIB licensing in advance, but a more permissive and somewhat less bureaucratic system, focusing more on sensitive uses of personal information, was introduced in the 1982 revision. The revised law was designed to reduce the bureaucratic burden of data protection and to make the system of selective licensing of personal information systems self-supporting. These revisions occurred in response to DIB's own internal assessment of what changes were necessary and the government general desire to reduce the costs of government. It is noteworthy that, because of Opposition fears of appearing to weaken data protection, the 1982 amendments passed by only one vote.

The Data Inspection Board has a Board of Directors, appointed for fixed terms, representing various political parties and interest groups, and a staff of less than 30. DIB exercises a great deal

[1] Material for this section was derived from David H. Flaherty, "Data Protection and Privacy: Comparative Policies," OTA contractor report, January 1985.

of power. It has the authority to control the collection and dissemination of personal data, to regulate the usages of the resulting register, and to set up a system of responsible keepers for computerized databanks. DIB also has the powers to investigate complaints, to inspect information systems, and to require information from organizations. The power of the cabinet or legislature to create a personal file outside the jurisdiction of DIB is an example of several safety valves in the legislation that prevent DIB from acting in a discretionary fashion on any specific measure.

The Data Act contains a few general data protection rules, for example, the data subject right of access and right to challenge are guaranteed in the act. But, DIB is responsible for designing detailed rules for particular systems and users, including what information may be collected, and the uses and disclosures of this information.

France

The 1978 Law on Informatics, Data Banks, and Freedoms is an expansive and innovative statute. Article 1 well illustrates this point:

> Informatics ought to be at the service of each citizen. Its development should occur in the context of international cooperation. It ought not to threaten human identity, the rights of man, private life, nor individual or public freedoms.

The 1978 law created an independent administrative agency with regulatory power, the National Commission on Informatics and Freedoms (CNIL). It is the first administrative agency in France with statutory independence from the government. CNIL is obliged to ensure the observance of the 1978 law and to make decisions on the authorization of particular information systems in response to requests. The Commission has 17 part-time members chosen for 5-year terms by various official government bodies, including the Senate, the National Assembly, the Council of State, the Court of Cessation, and the Court of Financial Accounts. There are also data protection officials in each government agency.

Critics argue that CNIL has never taken a tough decision against the government with respect to a proposed new personal information system. CNIL has rarely turned down a government proposal; it tends to negotiate changes during the process of application for approval. Because of the way it works in responding to specific requests for advice or licenses, CNIL has not yet reviewed in detail all of the databanks that existed prior to the enactment of the 1978 law.

United Kingdom

The Data Protection Act became law on July 12, 1984, and will gradually become fully operative over the next 3 years. The act established an independent Data Protection Registrar with a staff of 20 to 30 members who are not civil servants. They are to maintain a register of personal data users and computer bureaus in the public and private sectors. Although the Home Office emphasizes that the law requires simple registration of automated systems rather than licensing, as in Sweden and France, the act requires quite complete information on each system and the users of the system. It remains to be seen whether there are any practical differences in terms of the amount of paperwork required.

Canada

Part IV of the Canadian Human Rights Act of 1977 introduced principles of fair information practice for the Federal public sector and created the position of Privacy Commissioner. The powers of the Commissioner consisted primarily in responding to complaints from individuals about denials of individual access to government personal data. The current Privacy Commissioner was a member of the Canadian Human Rights Commission.

In 1982, the Federal Privacy Act supplanted and significantly strengthened the privacy provisions of the Human Rights Act. Sections 4 to 10 of the 1982 act regulate the collection, retention, disposal, protection, and disclosure of personal information held by the Federal Government by means of a code of fair information practices. Its provisions are similar to the American Privacy Act. The Canadian law also specifies a list of 13 purposes for which a government institution may disclose personal information.

The Treasury Board is responsible for publishing an annual index of all the personal information systems maintained by the Federal Government in both manual and automated form, including the fewer than 25 systems that are exempt from access by individuals. The current edition runs to about 300 pages. Copies are available in post offices and libraries across Canada, but it is unusual to find persons who have consulted them.

The 1982 Privacy Act considerably strengthened the general powers of investigation and monitoring, and set up a separate Office of the Privacy Commissioner. The Privacy Commissioner holds office for 7 years, and is eligible for reappointment

once. His independence is assured, in theory, by the fact that he is an officer of Parliament and is appointed by resolution of the Senate and House of Commons. In practice, the initial selection is in the hands of the government of the day; thereafter, the Privacy Commissioner has to retain the confidence of these two legislative bodies. Presently, the Information Commissioner, who is responsible for the law on access to government information, and the Privacy Commissioner share some administrative staff in the same office. The Privacy Commissioner has a legal advisor, a director of complaints and 5 investigators, and a director of compliance and 3 investigators, for a total of 15 direct staff and a share of 18 others.

The Privacy Commissioner has the overall responsibility to monitor the implementation of the Privacy Act. His recommendations to government departments are likely to carry a considerable amount of weight, although he does not have regulatory power, because he is an independent officer of Parliament. He can request a response from a department to one of his recommendations. He prepares an Annual Report to Parliament and may make special reports at his discretion. The act directs that a permanent committee of Parliament should review the administration of the statute. An individual may complain to the Privacy Commissioner about any alleged form of personal information misuse by the Federal Government. Moreover, the Commissioner has the power and resources to initiate and investigate a complaint himself.

Australia

In April 1976, the Australian Law Reform Commission was given a broad mandate to consider a variety of privacy issues, including data protection. After an exhaustive inquiry and the publication of a number of specialized reports, a comprehensive three-volume report was released at the end of 1983. With respect to its recommendations for data protection legislation, the Commission formulated 10 general principles for data protection modeled on the Organization for Economic Cooperation and Development's Guidelines. The Commission concluded that the private sector, as well as the public sector, should come within the ambit of legislation. It rejected the licensing model for data protection, but recommended the creation of a "statutory guardian" or "administrative body with the specific function of advocating privacy interests. " Such a Privacy Commissioner would function primarily as an ombudsman, but would have regulatory power in one specific area-the handling of individual requests to obtain access to their own data and to amend incorrect records. In general, the basic functions of the Australian Privacy Commissioner would be similar to those of his or her counterpart in Canada and data protection officials in Western Europe.

0

58-924 0 - 86