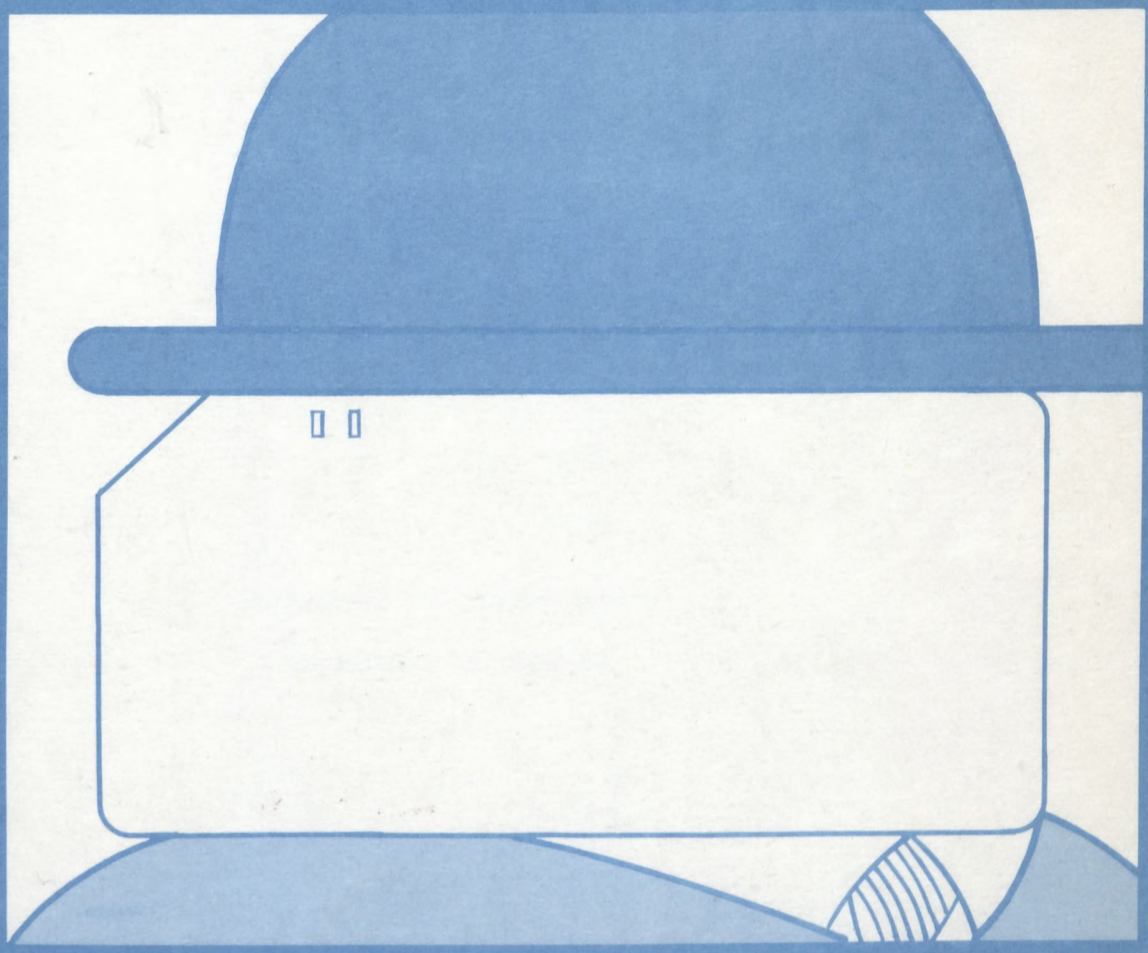
INTERNATIONAL FACTORS

C. DALFEN



A study by the Privacy and Computer Task Force

INTERNATIONAL FACTORS

A STUDY FOR THE

PRIVACY AND COMPUTERS TASK FORCE

DEPARTMENT OF COMMUNICATIONS

DEPARTMENT OF JUSTICE

C. Dalfen

This report was prepared for the Privacy and Computers Task Force, an inquiry sponsored by the Departments of Communications and Justice, and should not be construed as representing the views of any department or of the Federal Government. The views expressed herein are exclusively those of the authors, and no inference of any commitment for future action by any department or by the Federal Government should be taken from any recommendations contained herein.

This report is to be considered as a background working paper and no effort has been made to edit it for uniformity of terminology with other studies.

TABLE OF CONTENTS

Introduction

This study focuses primarily on data on Canadians which is collected, stored or disseminated outside the country, particularly in the United States which is the only foreign country in which significant quantities of data on Canadians are stored.

The study is divided into three sections. The first attempts to provide answers to four sets of questions relating to the quantity and types of data involved, and the mechanisms for its collection, storage and distribution. In the second, a description and analysis is provided of certain laws and practices in the U.S. and in Canada relating to data collection, storage and access. In the third section, the attempt is made both to identify potential problems facing Canada in connection with the international flow of data, and to suggest possible solutions in the domestic and international context.

In the Report of Telecommission Study 3(c) on the "International Legal Problems concerning the Transfer and Storage of Information", it was stated:

> ". . . it appears that definitive factual information about the numbers, types and owners of interconnections with foreign data banks, is (as with entirely domestic interconnections) extremely difficult to obtain. (The Dominion Bureau of Statistics informs us that they are not aware of any exhaustive up-to-date source of such information - government or otherwise). We must accordingly rely on examples that have come to our attention."[1]

---

1. Final Report, at p. 2.

Thanks to other studies in this Task Force, we have been slightly better able to penetrate the information barrier, but the problem of scarcity of detailed information on the subject still remains.

Our empirical base has three major sources:

(1) Thirteen answers received to letters of inquiry mailed to twenty-four U.S. concerns which were thought to have in their files personalized data regarding Canadians. These replies did not consistently address themselves to all the issues outlined above, resulting in certain gaps.

(2) Preliminary tabulations (tabulations of population variable) of the results of a survey questionnaire sent to some 2,400 enterprises.[2] Some 1,215 replies were received.

(3) Reports of some 43 site interviews of organizations holding large files of personal records in Canada. These interviews dealt for the most part with Canadian-based concerns.

The information provided by the above sources was not sufficiently broad and diverse to admit of strong generalizations on the subject. It has, however, yielded some useful preliminary observations.

---

2. The survey questionnaire was mailed by the Privacy and Computers Task Force under the imprint of the Departments of Communications and Justice, to 2,400 organizations. The mailing list was compiled from the Canadian Information Processing Society's current census of Computers, "Canadian Business" lists of the largest Canadian industrial and financial organizations, and membership lists of associations and organizations in fields including finance, health care, insurance, law enforcement, and social service, and federal and provincial government directories.

SECTION I - FACTS

QUESTION 1: Identifying the Data Banks:

Which U.S. data banks contain data on Canadians? What are the main types of data gathered in these banks? Who runs the data banks?

(A) U.S. Data Banks Relating to Credit and Loan Operations

(1) Credit Card Operations - Many U.S.-based travel-entertainment card companies (having some 235,000 Canadian citizens or residents as subscribers) operate in Canada. The information stored by these organizations includes the subscriber's name, address and other information supplied on his application form, including in some cases his employment history and references. As well, the data banks store information relating to the card holder's credit history with the firm.

(2) Loan Companies - Although full information is unavailable, it was reported that two U.S.-owned small loan companies are moving toward on-line lending in Canada which will rely on central data bases located in the U.S.

(3) Credit Reporting Agencies - A number of U.S.-based credit reporting organizations operate in Canada or provide services to Canadian customers. These agencies perform a wide range of services ranging from the computerized storage of credit card numbers and information on the status of each card to the storage of general credit information to the preparation

of credit reports on various corporations. For the most part, the credit information on Canadians stored by these firms remains in Canada.

(B) Insurance

Actuaries of some Canadian life insurance companies have links with computers in the U.S. for computation and actuarial information. An index maintained by a U.S. credit reporting agency and used by disability insurers to identify repeating claimants suspected of fraud, contains information on Canadians in its files.[3] The most important data bank, with files on some 800,000 Canadians, is maintained by an unincorporated association composed of both U.S. and Canadian Life insurance companies. The information stored consists mainly of coded medical information, but also includes sensitive non-medical information.[4]

(C) Law Enforcement

The R.C.M.P. feeds information (at present limited to data on stolen vehicles) into the U.S. National Crime Information Centre in Washington. Other non-computerized information is exchanged with various police forces, including the 105 national police forces which are members of Interpol.

(D) Taxation

There is a limited exchange of information between the U.S. Internal Revenue Service and the Department of National Revenue in accordance with Treaty obligations. This consists, for the most part, of the forwarding by

---

3. From Carroll, John M. "Personal Records: Procedures, Practices and Problems", p. 133. The number of subjects on whom information is maintained in the Index is over 9 million. In their reply to our survey questionnaire, the agency concerned stated that all the subjects were in the U.S.A.

4. Wheeler, S. "On Record: Files and Dossiers in American Life", Russell Sage Foundation, New York, 1969 at p. 210.

competent Canadian authorities to competent U.S. authorities on an annual basis the names and addresses of all persons whose addresses are within the U.S. (presumably including Canadians) and who derive from sources within Canada certain categories of income. At least one income tax consulting firm, a wholly owned subsidiary of a U.S. company, has in its files detailed taxation information on thousands of Canadians. However all such information remains in its Canadian offices.

(E) Other

Some U.S. controlled firms store non-computerized Canadian employment applications and management appraisal files containing extensive personal information in the U.S. At least one firm stores ultimate back-up tapes on all company files in the U.S. Four labour unions reported that all their files are located in the U.S.

The Survey Questionnaire Results:[5]

Although only 51% of the questionnaires were completed by the time the tabulations were made, the survey results nevertheless yield certain preliminary observations on the extent of information on Canadians stored in the U.S.

QUESTION 5A(1) - Physical Location of Records (Answered by 96% of respondents who provided completed questionnaires).

86 part of records in the U.S.

5 all of records in the U.S.

91, or 8% of respondents locate their records partially or entirely in the U.S.

---

5. The percentages cited below are taken from John M. Carroll's submission to the Privacy and Computers Task Force: "Personal Records: Procedures, Practices, and Problems", chapter 15, pp. 320 to 325.

QUESTION 5A(2) - Physical Location of Subjects or Client/Customers (Answered by 79%).

227 partly in the U.S.

10 entirely in the U.S.

237, or 25% of respondents have either part or all of their subjects, client/customers located in the U.S.

QUESTION 5A(3) - Physical Location of Information Recipients (Answered by 68%).

172 part of information disseminated to recipients in the U.S.

10 all of information disseminated to recipients in the U.S.

182, or 28% of the respondents have their information recipients partially or entirely within the U.S.

QUESTION 5B - Relationship with U.S. Based Suppliers of Information

481	never	)
381	occasionally	) supply information to U.S. based suppliers of information
61	frequently	)

383	never	)
441	occasionally	) obtain information from U.S. based information suppliers.
107	frequently	)

QUESTION 5(C) - "Have you ever seriously considered having portions of your data-processing operations performed in the U.S.?" was answered by 97% of those furnishing completed questionnaires. 151 concerns or 13% of the respondents, seriously considered sending information for electronic data processing to the U.S.

QUESTION 5D - "Under what conditions would you locate files in the U.S.?"

57 of some 1160 concerns replying to the question state that their files are now in the U.S. It is not clear whether this implies complete storage or partial storage.

Regrettably the firms which figured in the replies outlined above do not appear to have been contacted subsequently for more detailed information on the issues of our study.

QUESTION 2: Sources of Information for the Data Banks:

Who gathers and feeds the data on Canadians into the U.S. data banks? What sources of information are utilized?

(A) Data Banks Relating to Credit and Loan Operations

(1) Credit Card Operations - The bulk of the information is supplied by the card holder himself and the firms which have honoured the cards. In some cases local credit bureaus or the company's collection office may supply data.

(2) Credit Reporting Operations - The information gathered is generally supplied by the Canadian subjects themselves, including Canadian corporations. In some cases outside investigators may supply the data and records available to the public may be consulted.

(B) Insurance

The information on Canadians in the U.S. data bank maintained by Canadian and American life insurance companies is supplied by the 81 Canadian

companies and 9 regional underwriting offices which are members.[6] Similarly, the index used for identifying repeating claimants suspected of fraud relies on insurance companies for its information, although on occasion public records and the subject himself may be used as sources.

(C) Law Enforcement and (D) Taxation

The information is supplied by the R.C.M.P. and D.N.R. respectively.

Survey Questionnaire

The statistical tabulations do not distinguish between various categories of Canadian suppliers and therefore their value for this aspect is minimal.

QUESTION 3: Security Measures in U.S. Data Banks Governing the Storage of Data:

(A) Data Banks Relating to Credit and Loan Operations

Little information relating to security measures is available. Clearly, however, the precautions would seem to vary greatly. The largest organization of this type makes numerous steps to ensure the security of records, including computer passwords and identification codes and special security agents. Other companies' precautions are minimal.

(B) Insurance

Security procedures governing storage in the life insurance companies' data bank are closely supervised and there are many rules designed to ensure maximum privacy. All information is coded, companies desiring information must

---

6. The member companies currently write more than 90 per cent of life insurance issued in the United States and Canada and have more than 90 per cent of the life insurance assets in these countries. Wheeler, S. op. cit. at p. 208.

undergo identification procedures, and steps are taken to ensure adequate security provisions for the send and receive device at the company's office.

Survey Questionnaire

The tabulation of the survey questionnaire replies is of limited use in determining the extent of security measures in the U.S. Cross tabulations are necessary to determine whether any replies under questions 6A (adequacy of present safeguards) and 20A (measures employed to prevent unauthorized access) apply to operations in the U.S.

QUESTION 4: Access to the Data Banks:

(A) Data Banks Relating to Credit and Loan Operations

(1) Credit Card Operations - Generally the card holder is able to review and correct any information stored about him, and information is released to third parties only where there has been an application for credit and the company is given as a reference, or under court order. In the case of delinquent accounts access is given to a collection agency. In most cases access to the stored information is by way of telephone or mail; only one organization maintains remote terminals in its three U.S. operations centres, permitting direct access.

(2) Credit Reporting Operations - In all cases provision is made for the review of files, and the subjects, whether businesses or individuals, are free to clarify points or provide additional information. The subject is also entitled to know if information is released to

third parties, but there may be no systematic basis for informing him. Access to the information may be by telephone, mail or remote terminal.

(B) Insurance

The data contained in the life insurance companies' data bank is available only to other member life insurance companies and only after the applicant has applied to such companies for life or health insurance. The subjects only have access to non-medical information; and on occasion courts have been given access. The information contained in the index used to identify repeating claimants is supplied to insurance companies and evidently the agency which compiles it has a written policy regarding disclosure of personally identifiable information. The subject is entitled to examine all the data in his record.

(C) Law Enforcement and (D) Taxation

There is no information on access procedures relating to information stored in the U.S.

Survey Questionnaire

Preliminary tabulations of the survey questionnaire do not reveal information on access procedures of U.S. data banks.

Preliminary Observations on Section I:

Re Question 1: The majority of the American data banks examined in our study contain personal information used for making evaluative judgments on Canadians in connection with the granting of credit and loans. While containing the usual credit information such as employment history, past credit record, and references, they also often contain sensitive personal information not directly referring to credit. Most of the information is computerized and the number of Canadians who are subjects of the data runs into the hundreds of thousands.

The second major type of American data bank examined was that used for insurance purposes. Medical information for insurance purposes on at least 800,000 Canadians is stored in the U.S. and is mostly computerized. Information for insurance purposes also frequently includes sensitive personal information of a non-medical nature.

Data banks containing information on Canadians for taxation, employment, and law enforcement purposes appear minor in extent and import by comparison with those containing information for credit, loan, and insurance purposes.

The operations of a significant proportion of Canadian concerns involve the transfer of personal information on Canadians to the U.S. The preliminary state of statistical studies does not provide precise figures, however a rough guess based on the projections from the survey questionnaire would be from 10-25% of Canadian concerns.

Re Question 2: The major suppliers of personal information on Canadians to those U.S. data banks examined in our study are Canadian agents of American companies, Canadian credit companies, Canadian insurance companies and the subjects of the information themselves.

Re Question 3: Scant information was provided on security measures governing the storage of data on Canadians in the U.S. data banks.

Identification code numbers for persons accessing the banks and the coding of the data are the most common denominator in those security measures reported. The most elaborate security precautions were reported in the insurance field.

Re Question 4: Access:

Do Canadians have access to the data about themselves?

Most of the U.S. operators of the data banks relating to credit and loan operations contacted claimed that the Canadian subject can gain access to his file and correct or rebut information contained therein. In the insurance field, the major data bank examined only grants the subject access to non-medical information, but others apparently grant the subject access to all data in his record. Information is lacking on the access procedures instituted by those U.S. data banks operating in law enforcement, taxation, and other areas.

Is access sold to others or otherwise provided?

Eight data bank operators in the credit and loan field provided information on this aspect.

Apart from the common situations of release on court order, or release to collection agencies for delinquent accounts, half of the operators who responded utilize the information primarily for internal credit operations and restrict access to third parties to limited situations not involving the sale of the information of these concerns. Two restrict release primarily to those cases where they are submitted as credit references by the subject.

A third restricts release to its associates, and a fourth does not directly refer to release policy, stating only that the basic infile report supplied by the local credit bureau in Canada is used solely for the purpose of deciding on whether or not to issue a credit card.

Half of the operators in the credit and loan field release or sell information on Canadians to third parties on a broad scale. Vague criteria of eligibility for access are employed by these firms such as "need to know", "bona fide", "grantors of credit", etc.

In the insurance field, only two firms provide information on this aspect. One, not operated for profit, releases information only to those members to whom a Canadian applies for insurance. The other one, which is operated for profit, releases information to insurance companies.

Information was lacking on access procedures employed by U.S. data banks in other fields such as law enforcement and taxation.

What methods of access to data banks are there (mail, phone, etc.)?

Only five data bank operators in the credit and loan field gave information on this aspect.

Most of those data banks can be accessed by users through remote terminals. Access by subjects is for the most part by mail or phone.

The only other data bank giving clear information on this aspect uses teletypewriter devices or coded mail to access the central files.

Summary - Questions 1 - 4:

The fundamental point that emerges from the information available is that data about Canadians in U.S. data banks is treated no differently from data on Americans or on anyone else, in terms of information gathering procedures, storage security measures and access rules and requirements.

SECTION II - LAWS

1. U.S. Laws:

The regulation of storage and access to data in the U.S. is still in its infancy. No over-all regulatory body exists and no one law regulates all the various forms of data storage or access to it.

Since we are interested in data about Canadians, the crossing of state boundaries is involved (interstate commerce under the U.S. Constitution) and thus U.S. federal law is of prime relevance. Two Acts are of special importance for our study:

(A) The Fair Credit Reporting Act,[7] which regulates mainly the activities of U.S. credit bureaus, banks and insurance companies in the field of data collection, storage and distribution; and

(B) The Federal Report Act,[8] which regulates a large portion of U.S. government activity in this field. Both Acts are provided in the Appendix to this report.

The Fair Credit Reporting Act

The purpose of the Act is described in s. 1681(b) as being:

> "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this sub-chapter."

As this law has been in effect for less than a year, it is too soon to make an evaluation of the extent to which it safeguards the privacy of

---

7. 15 USC para. 1681 effective April 25, 1971.

8. Federal Report Act, 44 USC para. 3501.

Canadians who have data on them stored in U.S. data banks of the type considered in this report. This is especially so since the Act does not differentiate among the sources or the national origins of the data. It is premature to state categorically that the provisions of this law apply across the board to all aspects of the data bank activities we have outlined. It is curious that only one of the U.S. firms which were contacted made reference to it as governing their activities.[9]

Nevertheless, certain preliminary observations may be made.

(1) Storage

The Act applies to the collection and storage of data as follows:

(a) Notification: A "person" may not procure or cause to be prepared an "investigative consumer credit report" unless the subject is notified, and informed of his right to request disclosure of the nature and scope of the investigation requested, or the report is to be used for employment purposes for which the consumer has not specifically applied.[10]

Broadly speaking the Act refers to a person who prepares and issues a "consumer report" and its sub-type, the "investigative consumer report", as a "consumer reporting agency".

The definition given in the Act of a "consumer reporting agency" is so widely framed that it would cover almost any commercial data collector. It is defined at s. 1681a(f) as:

> "Any person which, for monetary fees, dues, or on a cooperative non-profit basis, regularly engages in whole or in part in the practice of assembling

---

9. One can assume, however, that the Act will cover most commercial personal data files. By virtue of s. 1681(S) the Act also applies to a wide range of banks, federal credit unions, common carriers in the transportation field, airlines and meat packers.

10. S. 1681d. Under s. 1681a(b) of the Act the term "person" means: "any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity".

> or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

Similarly the definition of an "investigative consumer credit report" at s. 1681(e) is sufficiently broad to encompass a wide range of personal information:

> "A consumer report containing information on a consumer's character, general reputation, personal characteristics, or mode of living (which) is obtained through personal interviews with neighbours, friends or associates ... (etc.) However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer."

(b) Prohibited information: In addition to the notification provisions relating to the collection, and impliedly the storage of "investigative consumer reports" there are detailed provisions relating to what may not go into a report:

- old information (except where the amount involved is substantial i.e. involving credit or life insurance of $50,000 or more or an annual salary of $20,000 or more).[11]
- s.1681K(2): public record information for employment purposes which has not been updated.
- s. 1681(1): adverse information in a previous investigative consumer report other than information of public

---

11. See s. 1681C on the prohibition of the reporting of obsolete information; different prescriptive periods are provided for different categories of information.

record unless such information has been verified, or has been received within 3 months prior to the completion of the subsequent report.

(c) Exclusions from provisions relating to storage: Although most of the collection and storage operations of many of the data banks included in our empirical base appear to fall under the aegis of the Fair Credit Reporting Act, the applicability of its provisions is narrowed by the following:

(i) The term "consumer report" does not, according to ss. 1681a(d) include:

> "... any report containing information solely as to transactions or experiences between the consumer and the person making the report".

(ii) A record, to fall under the definition of a "consumer report", has to be compiled by a "consumer reporting agency" and, according to s. 1681a(f), the latter must furnish these reports to third parties.

(iii) The "consumer reporting agency" must use a "means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports" (s. 1681a(f)).

(iv) The term "consumer report" does not, according to s. 1681a(d) include:

> "any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device."
>
> or
>
> "any report in which a person who has been

> requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under s. 1681m of this title."

(v) The term "investigative consumer report" does not include facts on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

Greater detail about the information on Canadians in U.S. data banks is required to determine the precise application to it of the Act and its exceptions.

(2) Access

The Fair Credit Reporting Act also provides access procedures for most of the types of data banks which contain data on Canadians.

The above-mentioned restrictions on the terms "consumer report", "consumer reporting agency", and "investigative consumer report" apply as well to the regulation by the Act of the access phase of data bank operations.

(a) Access by third parties: The effect of s. 1681b is to restrict access by third persons to "consumer reports" furnished by a "consumer reporting agency" to

- a court in the case of a valid court order
- those persons for whom the subject authorizes access

- to a person whom the consumer reporting agency has reason to believe will use the information for employment, insurance, or determination of government benefit, or "otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer."

It is the vagueness of the last category of persons to whom access may be given that constitutes the major defect of the Act in relation to the access phase of data bank operations.[12]

(b) Access by the subject: The law is also defective in its provisions relating to access by the subject of the data. S. 1681g provides for the subject to be granted, upon sufficient identification and on request, access to the nature and substance of the information contained in the file, the sources of the information, and the names of any credit grantors who have received a report on him during the preceding six months. (2 years, for employment purposes).

These provisions are defective in that

(i) they do not include medical information and therefore exclude a vast range of insurance information;

(ii) they generally do not include the sources of an "investigative consumer report", providing the sources were used solely for such report;

(iii) they do not apply to information received or consumer reports furnished prior to the effective date of the act unless they are contained in the files of the agency on that date.

---

12. The specific case of access by government agencies to specific identifying information held by a "consumer reporting agency" is covered by s. 1681f.

The Act sets out detailed procedures for access by the individual subject to the information contained in the files;[13] for the deletion of information which the subject disputes and which reinvestigation shows to be inaccurate; the notification to users of the deletion; and - where reinvestigation does not resolve the dispute - for the recording of the consumer's argument.[14]

The major deficiencies in these provisions are

(i) the individual can be charged a fee for exercising his rights (s. 1681j) if more than thirty days have elapsed from the time of his being made aware of the adverse use of the information to the time of his request;

(ii) it is not certain that sufficient means are provided to enable the individual to understand his record and his rights.

It is of prime significance for Canadians that such rights may be exercised by phone providing that there has been a prior written request (s. 1681h(b)(2)).

Most of the data bank operators which our study examined did not reveal any practice of informing the subject of the release of information to third parties. The Act (s. 1681m) goes some way towards remedying this situation by requiring that a user who denies the subject's request for credit, insurance, or employment, or increases the charge for credit or insurance because of information contained in a report, must notify the

---

13. See s. 1681h.

14. See 1681i.

subject of the decision and of the office which supplied the report. (Further as mentioned earlier, he can at all times, on request, obtain the names of the recipients of information in a 6-month period - (2 years for employment) - s. 1681(g)(3).)

Moreover, where a request for credit, insurance, or employment is denied because of information received from persons other than a consumer reporting agency the user must inform the subject that he has the right to request the nature of the information in order to challenge it.[15]

The Act provides stringent rules for its enforcement.

The law provides that

> "Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined not more than $5,000 or imprisoned not more than one year, or both (s. 1681q)."

It also provides that

> "Any officer or employee of a consumer reporting agency who knowingly or willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined not more than $5,000 or imprisoned not more than one year, or both." (s. 1681r)

There are also provisions respecting civil liability for wilful or negligent noncompliance with the Act (s. 1681n; 1681o).

(B) For those categories of data on Canadians held in U.S. government data banks the Federal Report Act applies.[16]

It provides some safeguards in that confidential information may only be released by one government agency to another government agency (a) in the form of statistical totals or (b) with the consent of the person(s) concerned

---

15. S. 1681m(b).

16. Apart from limited exchange of information for taxation purposes our study has not dealt with the data on Canadians held in U.S. government data banks. We have no information on its nature or extent.

or (c) if the receiving agency has authority to collect the information itself and the authority is supported by legal provision for criminal penalties against persons failing to supply the information. The recipient agency is under the same legal constraints as the agency which originally obtained the information. A further safeguard is provided by paragraph 3506 of the Act which provides for a hearing to determine the necessity for the information gathering of a particular government agency.[17]

Summary

Whatever advantages or deficiencies the U.S. law provides, it is clear that as in respect of the actual practice there is no differentiation made between the source or the national origin of the data concerned.

2. Canadian Laws:

There is no over-all Canadian federal Act dealing specifically or generally with the problem of privacy in the manner of the U.S. Federal Report Act, or Fair Credit Reporting Act. One or two, however, such as the Statistics Act, 1970-71 Statutes of Canada, c. 15, touch the problem peripherally. On the questions relating to the international flow and storage of data, there are no direct federal legislative provisions.

At the provincial level, only Manitoba, Ontario, Quebec and British Columbia have legislation dealing with certain aspects of the problem of privacy.[18] Only in Manitoba and Ontario, however, does the provincial legislation deal with the flow or storage of data beyond provincial boundaries.

(i) Manitoba

The Manitoba statute entitled The Personal Investigations Act (1971), (previously Manitoba Bill 27), regulates the gathering and divulging of information in Manitoba. It also provides for agencies and users outside Manitoba at section 11 of the Act, dealing with the verification of information.

17. Federal Report Act, 44 USC para. 3508.
18. The provincial Acts are the following: Manitoba: The Personal Investigations Act (1971) - Ontario: The Business Records Protection Act, R.S.O. 1970, c. 54; The Statistics Act, R.S.O. 1970, c.443; A Consumer Credit Reporting Bill was introduced in the 1971 session of the Ontario Legislature but lapsed with the end of the session. A modified Bill with similar objects is likely to be reintroduced before long. - Quebec: The Consumer Protection Act - British Columbia: The B.C. Privacy Act, S.B.C. 1968, c.39.

The section reads as follows:

> "Verification of information.
>
> 11. (1) Where the subject files a protest with a user or a personal reporter, or any person files a protest with a personal reporting agency, the user, personal reporter or personal investigation agency shall immediately
>
> (a) attempt to verify the information and where the factual or investigative information cannot be verified, expunge the information from the personal file; or
>
> (b) where the veracity of the information is sustained, record the protest in the personal file;
>
> and report the action taken
>
> (c) to the subject of the personal report or personal file; and
>
> (d) to any person to whom the personal report may have been furnished within the previous sixty days.
>
> Personal reporting agency outside Manitoba.
>
> 11. (2) Where a personal report is made by a personal reporting agency to a user in Manitoba and the office of the personal reporting agency is not located in the Province of Manitoba, the user is responsible for complying with subsection (1).
>
> User outside Manitoba.
>
> 11. (3) Where a personal reporting agency makes a report to a user whose office is located outside Manitoba, the personal reporting agency is responsible for complying with subsection (1)."

Section 12 then provides for an appeal if the subject is not satisfied with the action taken under s. 11, and s. 13 makes it an offence to fail or refuse to comply with any of the requirements.

Penalties for violation of any provision of the Act range from a minimum of fifty dollars to a maximum of two hundred dollars for an individual and from a minimum of five hundred dollars to a maximum of one thousand dollars for a corporation. If an individual or corporation is convicted again within one year the ranges are raised respectively to a minimum of two hundred and a maximum of five hundred and a minimum of one thousand and a maximum of two thousand five hundred dollars (s. 19).

(ii) Ontario:

There is at present no Ontario legislation of the extensive type in force in Manitoba.

The Business Records Protection Act, R.S.O. 1970, c. 54 provides in s. 1 that:

> "No person shall, pursuant to or under or in a manner that would be consistent with compliance with any requirement, order, direction or subpoena of any legislative, administrative or judicial authority in any jurisdiction outside Ontario, take or cause to be taken, send or cause to be sent or remove or cause to be removed from a point in Ontario to a point outside Ontario, any account, balance sheet, profit and loss statement or inventory or any resume or digest thereof or any other record, statement, report, or material in any way relating to any business carried on in Ontario, unless such taking, sending or removal, ... complies with certain requirements set out in ss. 1(a)-1(d)."

This Act relates directly to the question of dissemination of data outside the province and makes the violation of its provisions an offence punishable by up to one year's imprisonment (ss. 2(2), 2(3)). However, it must be noted that this Act applies only to information "relating to any business carried on in Ontario" and does not apply to data collected on extraprovincial businesses, or on individuals.

SECTION III - ASSESSMENT

On the basis of the information available, a number of observations can be made on the international flow of data on Canadians.

It is apparent that there are large amounts of data on Canadian individuals and associations stored in data banks in the United States, that this practice is found to be useful by Canadian businesses and professionals and that it will increase. At present no regulations inhibit this flow, or even record it.

It also appears to be the case that data stored in the U.S. on Canadians is not differentiated from that of any other origin but enjoys the same protection, or lack of protection, as any other data. In fact since U.S. law is more protective of the rights of people about whom data is stored and disseminated than is Canadian law, the ironic result is that Canadians appear to have greater protection when data on them is stored in the U.S. than when it is stored in Canada.[19] There appears also to be some spillover effect such that Canadian credit reporting agencies, usually subsidiaries or affiliates of U.S. organizations, apply the U.S. rules as corporate practice in Canada for purposes of standardization even though Canadian law does not require them to do so.[20]

The problem, then, is not, as one might have expected, that Canadians would be prejudiced by their data being stored in the U.S. It is rather that unless Canada enacts legislation - at both the federal and provincial levels -

---

19. As noted above, however, the U.S. Fair Credit Reporting Act has been in effect for less than a year and it is too soon to evaluate its effectiveness in safeguarding the privacy of Canadians or Americans.

20. Carroll, "Personal Records: Procedures, Practices and Problems", p. 89. This extends from the deletion of certain types of obsolete material to the right of a subject to discuss the content of his file with a Canadian branch manager and to refute unfavourable comments. It does not, however, extend to the right to be informed when an unfavourable report is circulated. (This situation has been changed in Manitoba with the passage of the Personal Investigations Act).

that is as protective of the data subject as in the U.S., it might well become a sort of "data haven" where U.S. and other foreign firms keep their data banks to evade the stricter requirements of U.S. law. This would prejudice both Canadian and foreign data subjects and could present a very undesirable image of Canada.

In the light of the present situation, what policy might Canada adopt regarding the storage of data about Canadian persons in foreign - particularly U.S. - data banks? Four options suggest themselves.

The first is to simply do nothing and rely on U.S. law to protect Canadians about whom data is stored abroad.

There are considerable disadvantages in this course. The problem of Canada becoming a possible "data haven" is one. Another is that U.S. law, which now provides greater protection for Canadians than does Canadian law, could change, leaving inadequate safeguards. More generally, it is not recommended practice to rely on the laws of foreign jurisdictions - over which Canada has no control - to implement Canadian policy or standards.

A second option would be to permit the continuation of the existing trans-border flow and storage but to require that companies in Canada storing data abroad register with the government or a registration authority. In addition, they might be required to notify the registration authority and possibly the persons concerned - each time data about them is stored abroad.

If a general Canadian internal policy of registration in the data field were adopted, this would accord with such a policy. It would permit

checks to be made and would give Canadian authorities up-to-date information about the nature and extent of data transferred and stored. On the other hand, it could be a somewhat cumbersome device.

A third possibility would be to carry this one step further and to require that a complete set of duplicate files be kept in Canada.

This would be an even more cumbersome procedure and might considerably compromise the value of storing data in a large central data bank abroad. Moreover, it might even be counterproductive, in that it might increase the risk of privacy being invaded, by having two locations at which data was stored and handled instead of one. On the other hand, it could possibly permit verification by Canadian subjects of the accuracy of the data of their facts.

Finally, and most extremely, there is the option of trying to prevent entirely the storage of data about Canadians abroad.

This option, however, would be undesirable in principle in that it would considerably hamper the flow of information essential to international commerce and the free exchange of information. Practically, it would be nearly impossible to enforce, given the many methods of transportation and communications for transferring information. Variants of this option, which would seek to curtail this flow by means of fiscal or excise regulations governing data would be subject to similar criticisms. As with regard to all options but the first, it is not certain that regulation of the transborder data flow is exclusively within federal jurisdiction. Significant loopholes could do considerable damage to the implementation of any federal policy.

Beyond domestic legislation, however, and since the U.S. is the principal state involved in this question for Canada, it might be desirable to explore the possibility of seeking a bilateral agreement on the storage of data by nationals of each country on the territory of the other. Such an agreement could provide for a commitment from each country not to withhold access by nationals of the other to data concerning them; it could provide for agreed standards of security for data banks; it could establish rules governing access to data by third parties, by courts, by information brokers, etc.; and it could provide for rules of verification.

Despite the advantages to this approach, there are certain difficulties raised which would have to be considered. These relate, inter alia, to the different degree of legal development in the matter of privacy as between the two countries, by different laws governing the admissibility of evidence in court, by Canada's own constitutional situation, by possible U.S. unwillingness to extricate the data question from the broader question of Canada-U.S. commerce, and by the existing state of Canada-U.S. commercial relations. It is, nevertheless, a possibility worth investigating further, which might even provide a useful spur to possible Canadian government policy in this field.

Apart from bilateral arrangements, it is also suggested that Canada ought seriously to examine the possibility of international arrangements relating to privacy and the international flow of data.

It appears clear that this flow ought not to be prevented or hindered both on the philosophical grounds that the free flow of information among countries is important in itself and on the practical grounds that people find it useful.

In order to safeguard privacy, however, the possibility of an international convention might be examined which, while it affirmed the desirability of the free flow of information, also embodied a set of model rules for the protection of persons about whom data is stored. This could both enhance national standards of privacy protection and encourage the compatibility of legislative provisions governing such protection in different jurisdictions. These rules might, as in the case of bilateral arrangements, though in perhaps a more general way, cover standards of data security, the right of access to one's file, the right of verification, rules governing third-party access, etc.

Such a convention would not only recognize the international implications of the question of computers and privacy but it could facilitate the free trans-border flow of information and could help to counter the arguments of those who would attempt to restrict the flow by arguing that Canadians would be subject to less effective protection if data about them were stored abroad.

It is clear that a large number of countries (including the U.S., U.K. and France) are currently conducting or are planning studies of computers and privacy. France, at a recent meeting of the OECD, stressed the importance of international compatibility in any domestic privacy legislation enacted. The International Union of Lawyers is conducting a study for the European Council of Ministers which will include draft articles for the protection of personal and industrial privacy. And the I.T.U. is likely to examine the question of privacy as far as the telecommunications links to data banks are concerned.

As mentioned above, one problem that Canada might have in respect of both multilateral and bilateral accords in this matter would be constitutional, in that the authority to implement certain provisions might well lie within provincial jurisdiction. In this area, as in the entire question of computers and privacy, federal-provincial cooperation is essential.

A second problem, at the policy level, concerns the need to view the question of computers and privacy as closely related to the total trans-border flow of goods, services, and business generally. One aspect of the question should not be artificially channelled out and dealt with in isolation from the mainstream of international commerce.

Above all, before any international initiatives are undertaken, it will be necessary to develop within Canada our own standards and mechanism for ensuring the privacy of our people.

STUDIES COMMISSIONED BY THE TASK FORCE

The Nature of Privacy - D.N. Weisstub and C.C. Gotlieb.

Personal Records: Procedures, Practices, and Problems - J.M. Carroll and J. Baudot, Carol Kirsh, J.I. Williams.

Electronic Banking Systems and Their Effects on Privacy - H.S. Gellman.

Technological Review of Computer/Communications.[1]

Systems Capacity for Data Security - C.C. Gotlieb and J.N.P. Hume.

Statistical Data Banks and Their Effects on Privacy - H.S. Gellman.

Legal Protection of Privacy - J.S. Williams.

Vie Privée et Ordinateur Dans le Droit de la Province du Québec - J. Boucher.

Regulation of Federal Data Banks - K. Katz.

Regulatory Models - J.M. Sharp.

Ordinateur et Vie Privée: Techniques et Contrôle - C. Fabien.

The Theory and Practice of Self-Regulation - S.J. Usprich.

Privacy, Computer Data Banks, Communications and the Constitution - F.J.E. Jordan.

International Factors - C. Dalfen.

[1] A joint Study by the Privacy and Computers Task Force and the Canadian Computer/Communications Task Force, to be published by the latter.