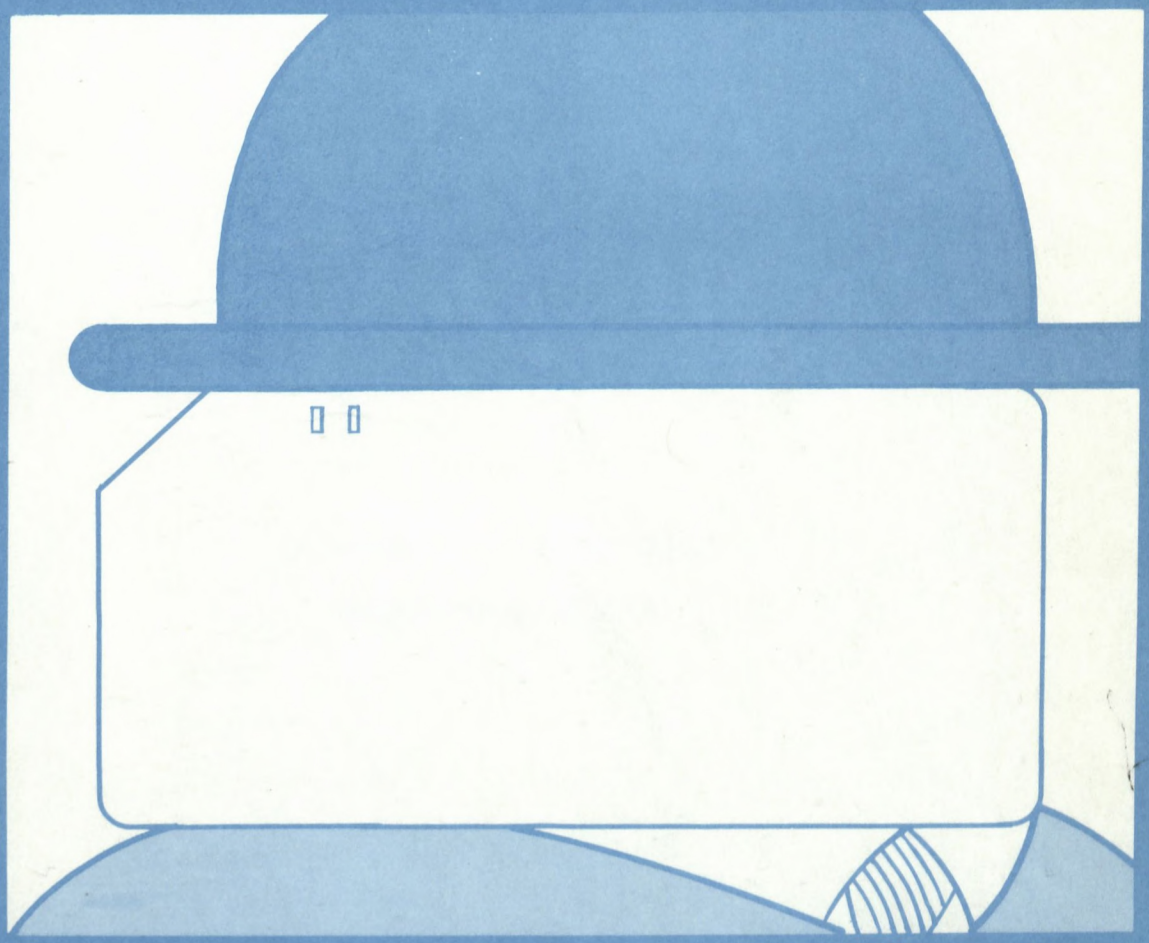
PERSONAL RECORDS: PROCEDURES PRACTICES AND PROBLEMS

J.M. CARROLL AND J. BAUDOT, CAROL KIRSH, J.I. WILLIAMS



3

A study by the Privacy and Computer Task Force

PERSONAL RECORDS: PROCEDURES, PRACTICES, AND PROBLEMS

A STUDY FOR THE

PRIVACY AND COMPUTERS TASK FORCE

DEPARTMENT OF COMMUNICATIONS

DEPARTMENT OF JUSTICE

J. Baudot
J.M. Carroll
C. Kirsh
J.I. Williams

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

CHAPTER 1

SUMMARY:

A study of personal records: procedures, practices, and problems in Canada was carried out between May and September 1971 by the Privacy and Computers Task Force.

The study consisted of the following major components.

1. Solicitation and analysis of briefs from Canadian Industrial and professional associations; 187 associations were approached. Briefs were received from 14 organizations. In addition, 32 of 200 briefs received by the Computer/Communications Task Force referred generally to the need for privacy and confidentiality of personal information and 22 made specific comments or recommendations on the subject.

2. Conduct of 43 site interviews of organizations holding large files of personal records. The interviews took place across Canada: from St. John's, Nfld. to Vancouver. They were selected so as to provide a representative sample from various functions within both the private and public sectors. Only one company, a computer dating service, declined to be interviewed.

3. A mail questionnaire was developed and presented with a mailing of 45 copies (15 in French and 30 in English). The pretest produced 24 replies. The final mailing of 2471 questionnaires produced 1268 replies (including pretest replies).

4. Letters of inquiry were mailed to two dozen American organizations which were thought to have in their files significant amounts of personalized data regarding Canadians. We received 13 replies; 8 said they hold such records, a total of 1,038,595 Canadian names. Four organizations did not know how many Canadian names were in their files; one reply was negative.

5. A search of print media was undertaken in Toronto, Montreal, and London for reports of alleged or actual invasions of individual privacy, and personal profiles were prepared of data thought to be in personalized files.

The investigative methodology is described in detail in Appendix I.

6. The study incorporates the major findings of a detailed study of the handling of student records in Canadian universities. This study, sponsored by the Canada Council, Social Sciences and Humanities Division was conducted by Carroll and Williams in 1970.

On the basis of the studies undertaken, the following general observations can be made:

1. An invisible college of information exchangers exists.

2. A lack of guidelines regarding information exchange creates a vacuous area in which wide discretionary power is wielded.

3. Any information system is as weak as its weakest link. For example:

   (a) low-paid and, on at least one occasion, loquacious enumerators used by Statistics Canada;

   (b) branch offices of large personal loan companies where customer applications are left in custody of low-grade clerks;

   (c) investigatory credit reporting firms in which major input comes from over-worked and ill-trained field staff;

   (d) government files sent about Ottawa in the custody of taxi drivers.

4. Standards of security are generally low; no system can guarantee the privacy of its subjects' information, if it cannot guarantee the integrity of its files.

5. There is much more data interchange than the public realizes -- principally because of the invisible college and lack of guidelines. For this reason:

   (a) an inaccurate item of data in one file will often reappear in a whole series of files;

   (b) information gathered with the subject's approval can later be used in other contexts, frequently to the subject's disadvantage.

6. Most information systems are local in a formal sense, but through information interchange are able to conduct operations on a national and international scale.

7. Analysis of mail questionnaire returns indicates there would be a ready acceptance of regulation on the part of those now operating personalized information systems.

CHAPTER 2

INTRODUCTION

The study of Privacy and the Computer is really the study of Man in relation to his environment in our post-industrial society.

The pristine concept of privacy as the right of an individual to determine what information concerning or describing him shall pass to whom, at what times, and by what means; and to what ultimate purposes it shall be put has been modified to a Social Contract. This contract requires that whenever an individual seeks a benefit or privilege, he may be obligated to furnish the grantor with facts about himself that will form the basis for judging his claim; and that society may gather such facts about individuals as it deems necessary for its proper functioning and for insuring the rights of others.

For his part, the individual may reasonably ask:

compassion, that the process of fact gathering does not inflict undue inconvenience upon himself, his family, or his intimate associates;

fairness, that no extraneous information is gathered or facts that may provide the basis for racial, religious or other unlawful discrimination;

accuracy, that information describes him correctly and does not improperly characterize him in an adverse manner;

confidentiality, that information about him is handled in confidence and not used for purposes the individual did not envision when it was gathered, and

forgiveness, a limitation on the time period during which derogatory information arising from events in the past can be used to the individual's detriment.

The title of this study is Privacy and the Computer. But the computer is merely an instrument, part of a larger information system. Moreover, no information system has any existence in its own right. For it too is just a tool by which some agency exerts control over its subjects, or provides them with benefits.

In this context, one cannot blame the computer alone for man's loss of privacy; that happened when man began to accept benefits from agencies and thus became subject to their adjudication and accounting.

Subjects have a dependency relationship with an agency, or a system of agencies. The dependency relationship may be synthetic -- that is, the agency may, in fact, depend for its existence on

the patronage of its subjects. However as long as the subjects perceive the services or requirements of the agency as beneficial or obligatory, the dependency relationship may be considered as valid.

The dependency relationship may be second order; in such cases the benefit the agency confers upon its subjects may simply be a favourable recommendation to a second agency. Thus the picture emerges of man as a subject of several agencies, which may in turn be privately or publicly owned. As a convenience in discussion, a group of agencies dealing with a common subject matter, for example, insurance or medical care, may be thought of as making up a system of agencies.

Furthermore, most systems of agencies interlock in their areas of concern and a decision regarding an individual is rarely made wholly within one system of agencies. (Application of factor analysis to interagency information transfer data obtained during site interviews aided in identification of clusters of interlocking agencies. See Appendix II). These major interlocking information systems are seen to have in common the aim of reducing risk on the part of portions of the establishment.

Most individuals come under scrutiny of interlocking information systems in connection with their selection for employment and, to a lesser extent, their selection for retention and promotion.

Employers want to reduce the risk of engaging unsuitable employees. Factor analysis shows that the information systems that determine one's eligibility for employment include law-enforcement, motor-vehicles bureaus, credit reporting agencies, educational institutions, census and taxation, as well as the employer. Questionnaire results show that major industrial employers received 4.60% of all personal information exchanged among agencies. Service industries received 4.81%; employment agencies 2.40%, and associations 3.45% (this category was heavily weighted with replies from labour unions). Thus 15.26% of personal information exchanged among organizations is utilized to decide the eligibility of individuals for employment.

Another interlocking complex of systems determines one's eligibility for consumer credit. Credit grantors want to avoid extending credit to individuals unable or perhaps unwilling to repay. Credit bureaus obtained 8.21% of personal information exchanged among organizations. Credit grantors, including banking and lending institutions, public utilities, merchandizing houses, oil companies, and investment services, alone received 26.83%.

A third complex is concerned with testing a subject's means or the extent of his personal resources, should he apply for certain social assistance benefits. Administrators of public funds intended to furnish sustenance, education, or medical care to those incapable of paying for these benefits require information to assure

themselves that applicants are truly deserving. Factor analysis shows the benfit means test system to include taxation authorities, welfare agencies, insurance companies, census, law-enforcement agencies, motor-vehicles bureaus, credit bureaus, employers, and health services. Social welfare agencies received 4.67% of all personal information exchanged among organizations. Charitable institutions received 5.55%.

A fourth complex establishes fitness to operate a motor vehicle. Factor analysis shows the right-to-drive information system to include law-enforcement agencies, motor-vehicles bureaus, health services, census, and credit bureaus. However, motor-vehicles bureaus obtained only 1/2 of one per cent of all personal data exchanged among organizations.

The fifth interlocking complex of systems is concerned with determining an individual's eligibility to purchase various kinds of insurance. Insurance companies want to avoid selling policies to individuals most likely to incur loss; in particular, companies handling automobile casualty insurance and provincial departments of transport are interested in getting excessively accident-prone drivers off the road. Factor analysis shows the insurance eligibility information system to include credit bureaus, insurance companies, motor-vehicles bureaus, health services, employers, welfare agencies, and educational institutions. Insurance companies received 5.35% of all personal information exchanged among agencies.

The sixth interlocking complex provides intake and monitoring for the criminal justice process. Criminal justice agencies want to identify potential law breakers and reduce the risk of recidivism by selecting candidates for probation and parole and monitoring their subsequent actions. Law-enforcement agencies received 7.68% of all personal information exchanged among agencies. In addition, regulatory agencies received 6.36%.

A seventh interlocking complex revealed by factor analysis might be called the social planning system. It includes census (principally Statistics Canada), health services, credit bureaus, employers, and educational institutions.

EXCHANGE OF PERSONAL DATA

It became apparent early in our study that one of the most common grievances against information systems containing personal data was that information obtained for one purpose frequently and without the subject's knowledge is used for totally different purposes. This information may, in the process, by collated with other information concerning the subject.

The direct way to arrive at a quantitative measure of the exchange of personalized information among various types of organizations classified according to function would have been to ask each questionnaire recipient how many items of information (i.e. inquiries regarding named individuals) are communicated annually to and from organizations in each of our 26 functional categories. A little probing during our preliminary site interviews convinced us that such a question was not likely to be answered by any significant number of organizations. The most frequent response we obtained when we posed the question orally was that most organizations just didn't know.

Accordingly we determined to get at the answer by an indirect approach.

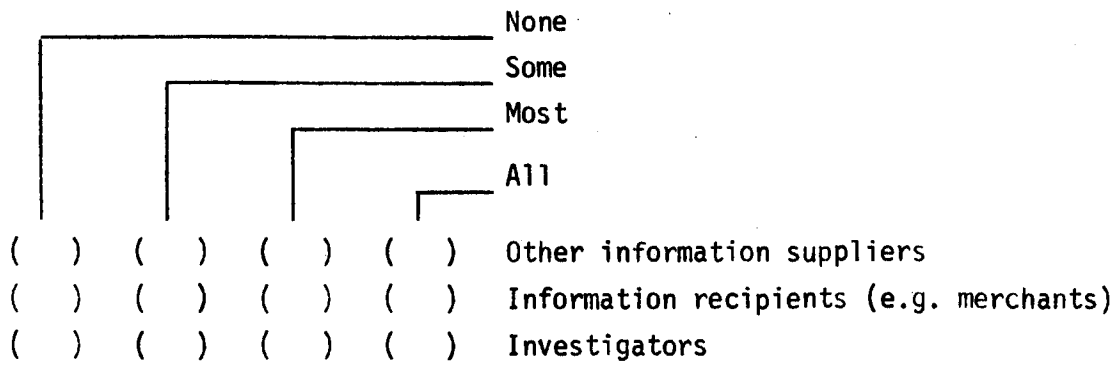
A quantitative measure of each respondent's activity as supplier of personalized information was obtained by the question:

"Please indicate the approximate average number of specific requests fulfilled annually?"

None	( )	1,000-10,000	( )
1-100	( )	Over 10,000	( )
100-1,000	( )		

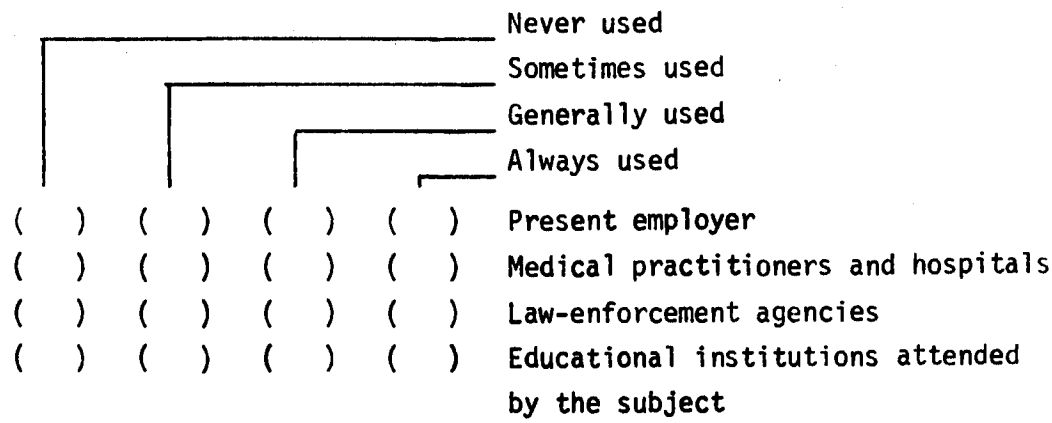
A measure of each respondent's activity in seeking personalized information from certain sources was obtained by the question:

"Indicate your principal means for gathering information for this file?"



and the question:

"Please indicate whether any of the following sources are used in collecting identified information about individuals for storage in your files?"



It was possible to identify each respondent with one of the seven categories postulated in the foregoing questions; that is, as an information recipient, information supplier, investigatory agency, employer, law-enforcement agency, health services, or educational institution. This identification was made on the basis of the functional category of the respondent organization. Thus, for the purpose of this study one would say that a bank functioned principally as an information recipient; a file-type credit bureau as an information supplier; and a private investigator, collection agency, or insurance adjustor as an investigatory agency.

The following functional types of organizations were characterized as being primarily information recipients; banking and lending institutions, insurance companies, public utilities, merchandizing houses, oil companies, investment services, and travel-and-entertainment card companies (credit grantors); also social welfare agencies and charitable institutions (welfare). The following types of organizations were characterized principally as being information suppliers: publishers and mass communications media, chattel mortgage (personal property security registration systems), credit bureaus, mailing-list suppliers, and market research firms. The following types of organizations were characterized as being primarily in the employment area: major industrial employers, service industries, employment agencies, and

associations (mostly labour unions). The following types of organizations were characterized principally as being in the enforcement area: law-enforcement agencies, regulatory agencies, and taxation. Health services, education, and the group: private investigators, collection agencies, insurance adjustors, etc., constituted groups of functional types in their own right.

Aggregating the replies to the question regarding annual inquiries answered over these seven categories, we have:

GROUP	NUMBER OF INQUIRIES	PER CENT
Information recipients	309,700	26.6
Information suppliers	98,300	8.4
Employment area	169,700	14.6
Enforcement area	49,000	4.2
Health services	320,000	27.4
Education	188,900	16.1
Investigators	31,000	2.7
	1,166,600	100.00

A quantitative measure of each respondent's utilization of an information source (utilization index) was obtained by weighting a response that said it was "always used" as equal to 3, "generally used" equal to 2, "sometimes used" equal to 1, and "never used" equal to zero.

The seven utilization indices (one for each category) were averaged over all seven categories, resulting in a 7 x 7 matrix of utilization indices. The upper left hand cell of this matrix, as an example, represented the utilization index of the group called "information recipients" as users of the source called "information recipients".

Utilization indices were normalized along each of the seven columns and the normalized utilization indices used to distribute the number of inquiries answered annually by the source represented by that column among the categories indicated by the row headings. (Note that this procedure implied that the respondents in each of the categories were equal in terms of their information seeking activity; that is, that our response base was truly representative of the Canadian information processing environment as it relates to records containing personalized inforamtion). Finally, all cell entries of the matrix were normalized with respect to the grand sum of the matrix (i.e. 1,166,600 inquiries annually).

The final matrix, shown below, depicts the information flow among seven categories of organizations. It enables one to say, for example, that law-enforcement agencies obtain 15.74% of all personalized information that is exchanged among organizations maintaining files of personal data, and that 3.70% is obtained from health services.

SOURCES OF PERSONAL INFORMATION

Seekers of Personal Information	Recipients	Suppliers	Employers	Enforcement	Health	Education	Investigators	Totals
Recipients								
Credit Grantors	8.95	2.43	4.34	.65	6.21	3.47	.78	26.83
Welfare	1.16	.82	1.14	.32	4.80	1.71	.27	10.22
Sub Total	10.11	3.25	5.48	.97	11.01	5.18	1.05	37.05
Suppliers	6.15	.86	2.30	.95	3.31	1.66	.22	15.45
Employers	2.95	1.21	3.02	.55	3.99	3.25	.29	15.26
Enforcement	3.00	1.91	2.10	1.08	3.70	3.22	.73	15.74
Health	.55	.39	.50	.20	3.18	.48	.12	5.42
Education	.95	.38	.43	.08	1.42	1.83	.03	5.12
Investigators	2.89	.41	.75	.36	.81	.48	.26	5.96
TOTALS	26.60	8.41	14.58	4.19	27.42	16.10	2.70	100.00

The striking thing about this matrix is that it indicated that personal information tended to flow towards certain repositories, which could potentially become very powerful factors in our society.

Health services and educational institutions appeared to give more information than they received by exchange with other institutions: 27.42 to 5.42 in the case of health services, and 16.10 to 5.12 in the case of educational institutions.

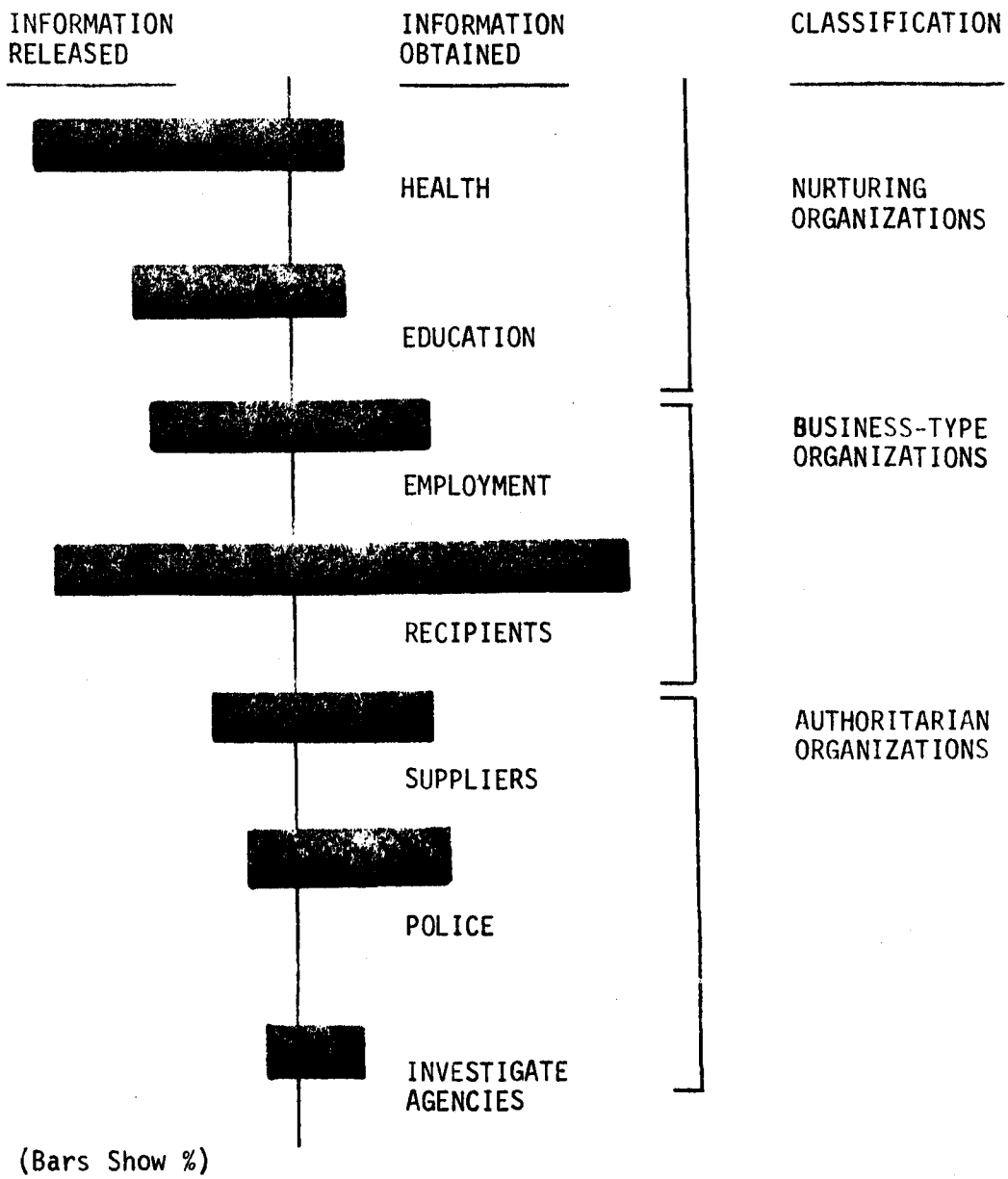
Employers gave just about as much as they received: 14.58 to 15.26.

Credit grantors and welfare agencies got somewhat more than they gave: 37.05 to 26.60.

However, information suppliers, law-enforcement agencies, and investigative organizations received far more information from other organizations than they gave in exchange. The ratios were 15.45 to 8.41, 15.74 to 4.19, and 5.96 to 2.70 respectively.

If knowledge can be said to represent power and knowledge of personal information to represent power over individuals, there appears to be a tendency for this power to become centralized in police forces, regulatory agencies, credit bureaus, private investigators, collection agencies, and the like, that is to say, organizations dedicated to acquiring and collating personally identifiable data concerning individuals.

THREE-WAY INFORMATION EXCHANGE MODEL



The bar graph illustrates that, with regard to the collection and dissemination of personalized information, organizations can be roughly grouped within one of three categories.

First there are organizations, usually concerned with the nurturing of the individual, which gather large amounts of personalized information in carrying out their legitimate functions and because of liberal or ill-defined policies with regard to disclosure of personalized information, or because of inadequate physical or procedural security measures, become sources of such information to other organizations -- some of which may have interests in conflict with those of the individuals concerned. In this first category we put health services, educational institutions, and, to a lesser extent, social welfare agencies.

Diametrically opposed to this first category is a second category of organizations usually concerned with exerting authority over the individual or with supplying information to third parties who may be concerned with exerting authority over him. These organizations make it their business to develop information regarding the individual, frequently by indirect means such as surveillance and importuning friends, neighbours, and relatives or by obtaining information from other organizations. In this second category we put information suppliers (such as in-file credit bureaus), law-enforcement agencies, and private-sector investigatory agencies.

The third category consists of organizations which have some clearly defined business relationship with the individual. These organizations gather such information about the individual as they perceive necessary to carry out their business functions and in so doing may exchange personalized information of this general type with other organizations in the same commercial area. In this third category we put credit grantors (banks, oil companies, merchanidizing houses), insurance companies, and employers.

This three-way model may help clarify the requirements for guidelines and instrumentalities to help preserve individual privacy of information.

1. With regard to nurturing organizations, there is need for enunciation and implementation of carefully defined and well publicized rules regarding dissemination of personalized information and establishment of electronic, physical, and procedural safeguards adequate to prevent these rules from being circumvented.

2. With regard to authoritarian organizations, there is need for enunciation of the rights of individuals with regard to these organizations and establishment of some mechanism to ensure, safeguard and assist the individual in implementing these rights -- whatever society perceives these rights to be with respect to each of the types of organization included in this category.

3. With regard to business-type organizations, need for intervention appears minimal except to the extent that patronage by business-type organizations of authoritarian organizations may foster practices which society may decide are against its best interests; and to the extent that what an organization perceives as legitimate business information may become defined by society as being intrusive upon individual privacy.

The dangers inherent in this increasing concentration of personal data in the hands of a few specialized organizations may have led the Canadian Manufacturer's Association to state in their brief:

> What is needed is legislation specifically directed to the problem of privacy which places suitable restrictions on the gathering, manipulation and distribution of information and which emposes high ethical standards on the people enpowered to use it.

And the Retail Council of Canada to say:

> It is the sale or other transmittal of (personal) information to third parties which may create the problem and we believe that it is in this area that review of procedures and study of possible contents should be concentrated.

Their brief went on to recommend that when information may be released to parties other than the organization which compiled it, individuals be given the right to check the accuracy of the factual elements of this information. The need for ensuring the federal accuracy of information in files is underscored because of the fact that most administrative decision-making systems are inferential. Basically, they attempted to predict future behaviour from past or present actions or situations with the help of statistically analyzed prior experience.

Although risk is reduced to the agency, two errors can be committed: some deserving individuals can be excluded, and some undeserving persons can be accepted. It is in the interests of society as a whole that the first type of error be reduced as close to zero as possible. There is a broader problem connected with selective processes. If no employer will take risk, then a hard-core population of unemployables will build up, whose sustenance will become a continuing burden to society as a whole; thus does the concept of forgiveness become an economic necessity.

Our study focussed upon information systems since the information system is at the heart of an agency's decision-making process with respect to its subjects.

Information is a ephemeral thing and studying information flow in the abstract is like studying fields and waves; one has to concentrate upon its visible surrogates. Thus we studied intake documents such as forms and questionnaires, their collation and reduction to records or dossiers, the accumulation of these records into files, the production of summaries and lists from files and their distribution, contacts between individuals whose business it is to acquire information, and the access of such individuals to files, documents, or reports.

An information system is centered upon its files but it must also include mechanisms for augmenting, updating, and correcting files and for retrieving information from them. Our interest focussed upon files having two essential characteristics:

1. they are now or potentially may become computerized, and

2. they are made up of records which are personally identifiable.

(It must be recognized that these two focus points correspond to the terms of reference of the Task Force. Many data banks containing highly sensitive information about identifiable individuals are maintained, and always will be maintained, in manual form).

Whether files become computerized or not depends upon several factors among which are the technical sophistication of the agency, its capital position, its management policy, the frequency with which its files are consulted or updated, the number of active records, and the structure of the files and the records comprising them.

All these factors are subject to some change, but the most dependable indicators of potential computerization are those relating to size, structure, and utilization. Roughly, a file of 10,000 records, 10% of which must be used or updated weekly, can be considered a candidate for computerization. Trade-offs between size and utilization are considered in deciding upon computerization. A small file with frequent access and a large file with infrequent access may have equal potential for profitable computerization.

As to structure, records must exhibit a common format, at least in identifiable subsets of the data items held on individual subjects. To be personally identifiable, records need not be sequenced on the subject's name; any unique identifier when indexed to the subject's name can serve as the entry mechanism to a file and make the information in it personally identifiable. Files which are frequently used to retrieve subsets of records sharing common values of selected data items are almost sure to become computerized at some time.

We examined in some detail seven aspirations of individuals that are adjudicated by highly institutionalized fact-gathering and record-keeping systems. These were employment, medical care, consumer credit, the privilege of operating motor-vehicles, education, insurance, and social assistance. Likewise, we addressed ourselves to three concerns of society that also rely on extensive fact-gathering and record-keeping. These were taxation, social planning, and the administration of criminal justice. We also studied the telecommunications networks and computing centres that implement the adjudicatory and real-time accounting systems. These studies formed the subject matter of the next 12 chapters of this report. They were based largely upon the results of site interviews conducted by the Task Force.

PRINCIPAL OBSERVATIONS (GENERAL)

The most serious potentials for invasion of individual privacy exist at the intestices of information systems. An invisible college of information exchangers exists that permits an agency to obtain bits and pieces of personalized information about its clients from other agencies; very few operational rules have been formulated to define or regulate this interchange.

In some cases, especially in government, the files belonging to several information systems share a common repository; in such cases the possibility exists for wholesale exchange of personalized information, and, again, no procedures have been formulated to regulate such exchanges.

There is, also, the pervasive influence of reporting agencies the activities of which, at present nearly wholly unregulated, cut broadly across practically all information systems.

Potentially contributory to unauthorized disclosure of personalized information is a general randomness in handling records and a lack of security consciousness among information-systems operators. This "hell-box" syndrome ("hell-box" is a newspaperman's name for a spare desk drawer into which he tosses any scrap of information he thinks may contribute to some future story) manifests itself in collection of irrelevant data, storage of obsolescent

information, casual handling of intake documents during the process creating records and a hard-copy (printed) output from computer files, and unwarranted reliance on the supposed security of data communications channels.

The hell-box syndrome is encountered principally in the information systems of non-profit institutions since cost consciousness, aside from considerations relating to individual privacy, tends to exert strong counter pressures on profit-seeking organizations.

The format of this report will be to examine each of the ten major systems with respect to their methods of acquiring personal information, the conditions under which it is stored, and the uses made of it. First, however, we are going to take a quick look at some principal invasions of individual privacy arising from causes that are not peculiar to any class of information systems but appear to afflict all of them to some extent. These instances are based upon events that have come to the attention of our investigative teams and do not draw upon the wealth of information previously published elsewhere.

The situations covered include the invisible college of information exchangers; the pervasive influence of investigative credit reporting agencies; random procedures for handling personal information at four nodes in a system: during its gathering and

collation into individually identifiable records; in the processing of these records, during their storage, and in the dissemination of reports made from these files; the vulnerability of computer systems to unauthorized interception of confidential information; and the storage of personal information concerning or describing Canadians in data systems beyond the reach of Canadian law.

The Invisible College -- Here are three examples that tend to indicate that informal contacts between information gatherers contribute to circulation of personalized information that goes beyond formal provisions for information interchange among organizations.

1. An unemployed man in Montreal complained to a government official that the collection arm of the local credit bureau was dunning him to pay on prior debts with unemployment compensation he had just received. The bureau, said the complainant, knew cheque numbers and amounts. A possible source of this confidential information could be traced to the fact that the local credit bureau is associated with a national investigative reporting agency, which does investigations for Canada Unemployment Insurance Commission.

2. An official of a casualty insurance company told us that, in Alberta, a provincial minister intervened with an automobile casualty insurance company on behalf of a young man who had been turned down. The insurance company was able to produce a transcript of the man's criminal record, which showed several convictions for narcotics offences including transporting contraband, the supposed confidentiality of criminal records notwithstanding.

3. A man in London informed us that he contracted with a lumber yard for a garage-stable and made a cash down payment intending to pay the rest with a savings balance to be transferred to his current account. He subsequently got a call from his bank manager, asking for his loan application. The individual stated that the lumber yard had called the bank, found that the customer did not have a balance in his current account sufficient to cover the entire sale, and wanted to know if he was going to borrow money to make up the difference. The customer protested to the accountant at the lumber yard who reportedly said that bank managers give him information about their customers current account balances "all the time". Current-account balances are supposed to be confidential.

Credit Reporting Agencies -- Investigative credit reporting agencies exert tremendous influence on employment selection, inspection of insurance applications, and evaluation of credit risks. But how reliable are they? Their field representatives work hard, conducting up to 16-17 interviews daily as well as writing up their cases. We were told during a site visit the average pay for full-time employees was $700 a month; however, some were part-time employees, and a considerable percentage were relatively new on the job. In their brief to the Task Force, Retail Credit of Canada Limited, said that in 1969 they employed 675 full-time salaried personnel and that their annual payroll was $3,361,000. Fifty-one per cent of staff had less than five years experience.

The president of a large casualty insurance group commented "They (investigative credit agencies) are as reliable as their field representatives let them be. They (the field representatives) are a mixed bag. Some are crackerjacks, but these men work full time on big life (inspecting applications for life insurance policies with high face value). Big life makes their profits, but auto casualty pays the rent. We had a case in Montreal; a customer was turned down for auto insurance and his insurance agent had sense enough to protest. The field representative had written his report on a neighbour living diagonally opposite; the neighbour was a lush. Of course, the applicant got his policy and the agent got a big pat on the back from me."

The principal credit reporting agency in Canada is Retail Credit Company of Canada Ltd., a wholly owned subsidiary of Retail Credit Company of Atlanta, Georgia. Traditionally RCC has been an investigatory credit reporting agency, but recently has been expanding its operations in the field of file-based credit reporting in both the U.S. and Canada. In the U.S. further takeovers of file-based credit bureaus have been enjoined under terms of U.S. Anti-trust legislation (similar to the Canada Combines Investigation Act). Although RCC files relating to its personal investigation activities, and indeed all its files in Canada, are kept in manual form, the U.S. parent company told us:

> Our subsidiaries have computerized credit bureau files in the Southeastern States and in the Pacific Coast States.

RCC has taken over several formerly Canadian owned file-based credit reporting agencies, the latest being the Credit Bureau of London, sold on Wednesday, December 15, 1971. Retail Credit Company of Canada Ltd. now owns, through its wholly owned subsidiary the Retail Credit Bureau of Montreal, credit bureaus in Trois Rivieres and Sherbrooke, Quebec; Winnipeg; Calgary; and Sydney, Nova Scotia in addition to the London bureau.

Random Procedures (Intake) -- Staff who gather information and get it into the files are often serious leaks.

1. Take, for example, the loquacious enumerator. During the 1971 census, an enumerator spent a quarter of an hour gossiping with the wife of one of our investigators. He named people, dates, places, who married whom and why they had to get married -- just about all the gossip in a village of 500. Reports in nationally circulated newspapers indicate that this was by no means an isolated incident.

2. A provincial health care plan reported that it discharged a clerk who met a friend at a party and commented "I haven't seen many claims from you lately." A psychiatrist told one of our investigators that another clerk was able to recite a list of his patients. Several doctors in this province now mail their claims directly to the executive director of the plan with the notation "call me for diagnosis."

3. National Revenue hires 1,000 housewives to keypunch tax returns during peak return period. Measures are taken to prevent them seeking returns of their friends, but these measures are not entirely successful. These part-time keypunchers do see tax returns of people they know and do gossip about their contents.

Random Procedures (Processing) -- Sometimes responsibility for processing is delegated and as a Latin maxim goes, "delegatus non potest delegare" (the delegate cannot delegate) -- but they do.

The federal government's Computer Services Bureau processes data for agencies that do not have computers and handles overload for agencies that do. When CSB itself is overloaded, it subcontracts to private firms. One federal agency (according to a senior official) was processing some confidential data for an African country; it was sent to CSB and was contracted to an outside firm. The original agency became concerned, especially when no record of this firm could be found. The agency official recounted that subsequently it developed that the firm was fictitious; it consisted of two professors moonlighting with the University of Ottawa's computer.

Before sending records to CSB for processing the National Parole Board takes the precautionary step of removing destination information from the records concerning notorious convicts.

Random Procedures (Storage) --

1. At a major psychiatric hospital, three patient records were missing at the time of our visit. Staff could not account for them.

2. A spot visit by our team to a 63-bed small-city hospital showed 15 obstetrical records improperly off premises; a doctor got behind in writing up his discharge summaries and took the records home.

3. Sensitive files in open filing cabinets are by no means unusual. One executive search firm we visited stated that it keeps its applicant files that way although the after-hours cleaning staff is hired on a transient basis by an outside contractor.

4. In one Toronto insurance company, files of declined applications were stored in unlocked filing cabinets, in the basement lunchroom used by female staff. There was thus no physical barrier to prevent the staff reading confidential investigative credit reports containing sensitive information.

Random Procedures (Dissemination) -- Broadside dissemination or lack of accountability for hard copy printout of computer files can result in leaks.

1. In one city, the municipal welfare department circulated 15 copies of their welfare records among various city agencies.

2. In one province an official of a government data processing facility left to become a university professor. He stated to us that he took with him the high school and college records of all students in the province, as data for a personal study project.

3. On May 17, 1971 we wrote to the RCMP asking about the proposed policy of transmitting complete criminal records over the proposed Canadian Police Information Centre system. We asked "what restrictions are proposed to prevent co-operative Police Forces from building up ad hoc files from teletype print-outs of Criminal Records, which files might be held under conditions of dubious security." Their reply dated June 18, stated among other things that "The comment that files retained by police forces may be held under conditions of dubious security cannot be accepted." On July 17 the Canadian Press reported that 40 or 50 RCMP files on paid informers had been stolen on May 6 from an unguarded RCMP station at Long Sault, Ontario.

Over-Reliance on Technology

Some information systems managers, on the basis of evidence collected, fail to understand the peculiar hazards of the computer age.

1. Officials in Ottawa advised us that a common way of sending a magnetic tape file from one government agency in Ottawa to another is to have it delivered by taxi. Should the driver, for one reason or another, decide to detour by way of a computing centre controlled by adverse interests, it would require only seven minutes to copy a 2,400-foot reel of tape.

2. Telecomputing brings with it special problems. We were informed that a "bomb out" or massive disclosure of data occurred at a private Ottawa computer bureau that provides remote teleprocessing services. A highly sensitive file belonging to one federal agency was erroneously printed out from temporary storage onto a remote printer belonging to another user. Luckily the other user was another federal agency; it could have been any of 20 remote terminal users, some commercial companies and some located in the U.S. (Data in temporary storage is now encrypted, we were advised).

3. The ease of wiretapping on data communications is not fully appreciated. Whether such activity is even illegal under the proposed antiwiretapping legislation is a moot point. A compelling argument against transmitting confidential data over telecommunications lines is that Bell Canada itself does not transmit its own confidential data that way.

In their brief to the Task Force, the Telephone Association of Canada said:

> The need for new security measures will evolve. Such measures should be provided on a discriminatory basis so that the degree of security and its cost is as closely as possible related to a specific need. Moreover, let us ensure that in trying to protect privacy for some, we do not invade it for others. As a result of this need for balanced judgment there will develop an hierarchy of communication/computer security measures. These will involve both technological and procedural safeguards.

Data Outside of Canada -- It may already be too late to achieve viable controls over traffic in some personally identifiable information concerning Canadians; a lot of it is no longer in Canada. In their brief to the Task Force, the Ontario Medical Association raised questions regarding the problem of foreign-based data centres. If laws are ever devised to provide in Canada rights of privacy and of information and recourse for the aggrieved, how could such laws be enforced in another jurisdiction? For example, analysis of patient answers to a long questionnaire may form the basis of a report suggesting that the patient shows evidence of mental illness. At least one such questionnaire may be sent to a laboratory in California where it is interpreted with the aid of a computer.

Other specific examples that have come to the attention of the Task Force included the following:

1. If you apply for a life insurance, the company will verify whether you have ever been turned down or rated by another company. The file they check is the Medical Information Bureau and its data base is in Boston, Massachusetts.

2. If you apply for disability insurance, the company will verify whether you are a chronic malingerer. The file they check is the Casualty Index and its data base is in Morristown, New Jersey.

3. If you make a credit card purchase in excess of fifteen dollars at certain gas stations, the attendant will call a toll-free number in Toronto to find out whether your account is delinquent or if the card you present has been stolen. The Toronto operator uses a remote terminal to query a data base maintained by National Data Corporation in Atlanta, Georgia to find out.

4. If you apply for credit, some grantors will query the Credit Index, a list of nine million defaulters. Its data base is in Morristown, New Jersey.

5. Two finance companies doing on-line lending in Canada check your credit by querying data bases in the United States.

6. Employees of brokerage houses that are members of the New York Stock Exchange who purchase stock in their company are investigated as to places lived, schools attended, and jobs held since age six. This information is kept by the NYSE. At least one Canadian brokerage house is questioning the value of a seat on the NYSE in view of these and other requirements.

OBSERVATIONS - SITE VISITS

The men we spoke to during some 50 site interviews were all sincere men of good will. All could give what they considered to be valid reasons for every bit of data collected and most could describe in detail measures taken to protect the privacy and confidentiality of personal information. Based on public speeches at conventions and the like, computer scientists seem to be more aware of the power of the computer as a potential mechanism to invade privacy than professionals from other disciplines. Only the social scientists, still enjoying very much their professional honeymoon with the computer, seemed so dazzled with its ability to manipulate statistical data as to be somewhat blind to its more sinister potentialities. But the fact remains, taking our work in total, that the average Canadian enjoys privacy only within restricted limits, and that his personal living space is under attack.

No concrete evidence was developed nor was looked for to determine the attitude of the Canadian public, that is, whether they were aware of the threats to their privacy, or cared about them.

The point is -- it is not how information is used today, or how it is gathered, whether the investigator takes off his hat when he talks to you or not, but just the fact that it is on file and can be used, exchanged, and collated with other files, which constitutes the potential danger to freedom.

The truth, as contrasted with fact, is that you can no more measure and analyze privacy than you can any other essential part of the quality of life -- like the beauty of a woman, or the love of a mother or the warmth of a home. The mere number of records held in files, the size of these records, the amount of sensitive -- at least as perceived by human beings if not always by the illuminati -- data contained in those files, coupled with evidence that some information has leaked into unauthorized hands and that some persons have been hurt, should demonstrate the existence of a significant threat to privacy except to those who choose to be blind and thus promote their self interest, or who indeed doubt that any right to privacy exists at all.

There can be no doubt that the computer, if not, as an inanimate machine, the cause the erosion of privacy, is nevertheless certainly guilty of aiding and abetting. Use of computers will be essential to retrieval and exchange of personal data in the future, even if many of the most serious invasions of privacy today arise from manually operated systems. The computer is also a highly visible and convenient target at which to direct measures for regulation and control.

No class of organizations is without some shortcomings with regard to preservation of individual privacy. All have dangers peculiar to them. Non-profit institutions are dangerous because of their random procedures. Government is dangerous because of its sovereign power. Industry is dangerous because its profit motivation may tend to obscure the rights of the individual. And when information systems combine organizations from two or more classes, the potential for damage to an individual is increased sharply.

The insurance super-system is a case at point. All three systems are at work here: we see the profit motivation of the insurance companies themselves, the power of the police and the motor-vehicle bureaus, and the random procedures of medical systems that allow their files to be penetrated for personal information, combine to jeopardize the interests of the individual.

OBSERVATIONS - SURVEY QUESTIONNAIRE

The principal investigative tool used by the Privacy and Computers Task Force in its study of procedures, practices and problems related to records containing personally identifiable information was a questionnaire mailed under the joint imprint of the Department of Communications and the Department of Justice to 2,516 Canadian-based organizations. The structure of this questionnaire, its development and testing, the characteristics of the sample, and a detailed analysis of results, will be given in Chapter 15. Only the more significant results will be discussed here.

A total of 1,268 replies were received; a 50.4% response. However, not all respondents completed the entire questionnaire. Therefore, the response base varied depending upon the question.

The responding organizations employed nearly 1.2 million persons; one sixth of the Canadian labour force. Of the organizations responding to the questionnaire, 55 listed themselves as federal agencies. Thirteen of these described themselves as social welfare agencies; nine said they were concerned with health or vital statistics. A number of unique federal agencies were missing from the response base. They received site visits from the Task Force, which will be reported elsewhere in this report. These agencies included Statistics Canada, National Revenue-Taxation, National

Health and Welfare, Public Service Commission, RCM Police, Canadian Penitentiaries Service, and National Parole Board.

There were 146 provincial agencies in the response base including 38 in the health and vital statistics field, 17 educational institutions, 11 public utilities, and 9 social welfare agencies. Only two taxing authorities responded and two motor-vehicle bureaus. However, the Task Force made a site visit to the Manitoba Motor Vehicles Branch. The report also drew upon an in-depth study by Carroll and Williams of the handling of student records in Canadian universities (1970).

Of 73 municipal agencies responding, 16 were concerned with health and vital statistics, 8 with social welfare and 7 with education. Out of 11 law-enforcement agencies responding, 5 were municipal police forces.

There were 302 federally incorporated organizations responding. Of these, 89 were industries, 37 insurance companies, 19 banking and lending institutions, 19 service industries, 18 associations, 15 oil companies, 13 charitable institutions, and 11 merchandizing houses.

There were 502 provincially incorporated organizations; 94 health services, 47 investment services, 37 educational institutions, 33 industry, 33 banking and lending, 33 private investigators or collection agencies, 29 associations, 22 charitable institutions, 14 insurance companies and 6 credit bureaus.

Of the 33 foreign incorporated organizations responding, 19 were insurance companies and 4 were labour unions.

Otherwise, 55 respondents did not characterize themselves, with respect to legal structure, and 102 listed themselves in the "other" category.

Classified by function, respondents included:

182 Health services,

127 Major industrial employers,

95 Associations,

83 Service industries,

76 Insurance companies,

76 Educational institutions,

64 Investment services,

61 Banking and lending institutions,

54 Charitable institutions,

43 Private investigators and collection agencies,

39 Social welfare agencies,

38 Public utilities

22 Merchandizing houses,

22 Oil companies.

Responses were received from 11 law-enforcement agencies, 11 employment agencies, 10 credit bureaus, 8 publishers, and 7 regulatory agencies. The credit bureaus responding were file-based organizations, but the Task Force made site visits to two major investigatory credit bureaus.

Two responses each were received from motor-vehicle bureaus, taxing authorities, travel-and-entertainment card companies, and mailing-list suppliers. One response was received from an organization engaged in chattel mortgage registration and a market-research firm. However, the Task Force made a site visit to Ontario's Personal Property Security Registration System.

In addition 36 respondents did not indicate their function and 193 listed themselves in the "other" category.

As to organizational objectives, 622 respondents characterized themselves as profit-making, 616 as non-profit; 30 did not answer this question.

TECHNICAL CHARACTERISTICS

About 43% of the responding organizations used computers to process files containing personal data. The following functional categories of organizations appeared most likely to have computerized their files containing personal data: public utilities, educational institutions, insurance companies, major industrial employers, oil companies, merchandizing houses, investment brokers, publishers, and banking and lending institutions. In addition, both of two motor-vehicle bureaus and one of two taxing authorities responding said they had computerized records containing personal data.

Of the computer users, 61% controlled their own computers. The remainder used the facilities of computer service bureaus or computer utilities. Organizations in the health and investment services fields tended to use outside facilities, rather than their own computers.

Forty per cent of organizations operating their own computers reported having remote-access provisions.

Only 4% of the computer users said they were processing personal data prior to 1955 - principally major industrial employers and insurance companies. Ten per cent said they started during the years 1955 to 1960. Twenty-one per cent began during the period

from 1960 to 1964 - oil companies and investment services reached their peak in this period. Between 1964 and 1969, 49% of the computer users began processing personal data. All other types of organization reached high points of computerization during this period; except for service industries, which were still increasing their use of computers in the post 1969 years. Sixteen per cent of computer users started during the period from 1969 onward.

On the basis of the Task Force study, there appeared to be a slowing down of new computer applications in the business data processing field. Whether this was due to a temporary scarcity of investment capital or whether it represented a saturation of the existing computer market cannot be determined from the facts developed in this study.

Most computer users (59%) had machines in the range of 64,000 to 256,000 words of core memory -- reasonably large-scale computers. Another 34% had machines of larger core memory capacity. Only 7% used smaller machines as their principal data processing computers.

OPERATING CHARACTERISTICS

The study recognized three basic kinds of files containing personally identifiable information. The first concerned the organization's own employees. The second concerned the organization's clients or customers; instructions to respondents requested that patients, students, policy holders, and members be included in this category. The final category concerned subjects, defined to include prospective customers, persons upon whom credit and criminal records are held, automobile registrants and licencees, and research subjects.

In general, respondents followed instructions. However, analysis of 722 questionnaires revealed that some organizations were confused; viz:

FILE REPORTED \ CATEGORY ASSIGNED BY RESPONDENT	EMPLOYEES	CUSTOMERS	SUBJECTS
Subjects	20	49	34
Clients	15	64	6
Customers	16	78	0
Patients	25	111	13
Employees	129	14	4
Students	4	30	6
Members	21	52	31

Four classifications of file size by number of records were established: 1-5,000; 5,000-50,000; 50,000-500,000; and over 500,000. The following table shows how the files reported upon were distributed according to number of records.

CATEGORY / FILE SIZE	EMPLOYEES	CUSTOMERS	SUBJECTS	
1-5,000	326	284	93	703
5,000-50,000	83	174	29	286
50,000-500,000	8	151	23	182
Over 500,000	0	36	18	54
	417	645	163	1,225

As to computerization: 40% of employee files containing 500 or fewer records were computerized while 76% of employee files containing more than 500 records were computerized; 54% of customer files containing fewer than 2,000 records were computerized while 81% of customer files containing more than 2,000 records were computerized; and 36% of subject files containing fewer than 25,000 records were computerized while 47% of subject files containing more than 25,000 records were computerized. Both file size and purpose are determinants of computerization. Customer files were most likely to become computerized. Subject files were least likely, probably because of the more narrative information often incorporated in them.

LOCATION OF FILES

Only five organizations said they had all their files in the U.S. and four of them were labour unions. Sixty-six per cent of all files containing personal data were located within the particular province in which the organization operated. Twenty-six per cent of the files were located elsewhere within Canada. Eight per cent were wholly or partially in the U.S. Aside from labour unions, the organizations most likely to have files wholly or partially in the U.S. were oil companies, insurance companies, health services, manufacturers, and lending institutions. Health services had files in the U.S. largely because they contributed to continental clinical data banks.

On the other hand, 76% of respondents said they would never locate files in the U.S. The rest said they would, if it were to their advantage to do so and, of course, some had files already there.

Forty-eight per cent said they furnished personal data to recipients in the U.S. The types of organization most likely to do so were credit bureaus, regulatory agencies, law-enforcement agencies, major industrial employers, insurance companies, merchandizing houses, and employment agencies. Both of the mailing-list suppliers and motor-vehicle bureaus responding said they furnished data to U.S. recipients.

Fifty-nine per cent of respondents said they obtain personal data from U.S. suppliers.

COMPUTER EXPERIENCE

The response base was, of course, narrowed to the order of 500 when analyzing responses to questions regarding experiences of organizations that were utilizing computers to do business data processing.

Seventy-five per cent said the most sensitive and confidential personal data was still held in manual form.

Only 26% said that computerization had resulted in greater centralization of personal data.

Seventy-four per cent said that errors were detected during the process of converting manual files to EDP format.

INFORMATION SOURCES

The subject himself was the most commonly used source of personal information; 88% of respondents said they regularly (generally or always) used the subject as a source. The second most frequently used source was hospitals and medical practitioners -- 34%. In contrast, only 30% regularly checked references named by the subject; 24% obtained information from his employer; and 21% obtained information from educational institutions he had attended.

The types of organization most likely to seek personal data regarding subjects from hospitals and medical practitioners were health services, insurance companies, social welfare agencies, charitable institutions, regulatory agencies, and major industrial employers. The one personal property security registration system (chattel mortgage) responding said it generally consulted this source.

Thirty-one per cent of respondents said they made some use of investigators in gathering information about the subject. The types of organization most likely to do this were law-enforcement agencies, insurance companies, collection agencies, social welfare agencies, regulatory agencies, credit bureaus, merchandizing houses, and major industrial employers.

The organizations most likely to receive complaints regarding their methods of collecting personal data were: law-enforcement agencies, credit bureaus, insurance companies, social welfare agencies, oil companies, and educational institutions. One each of the two motor-vehicle bureaus and two travel-and-entertainment card companies responding reported receiving complaints of this nature.

The five organizations most frequently complained about included an insurance company, insurance adjustor, private investigator, social welfare agency, and a police force.

RULES

Thirty-nine per cent of respondents said they made personal data available outside their own organizations. In 57% of cases these data were said to deal with customers; in 28% of cases with employees; and in 15% of cases with subjects. In terms of files held, the percentages were 55, 31 and 14.

Organizations most likely to release personal data outside their own organizations included regulatory agencies, educational institutions, credit bureaus, health services, insurance companies, oil companies, and law-enforcement agencies. Both of the motor-vehicle bureaus responding said they release data outside their own organizations.

The organizations most likely to receive complaints regarding disclosure of personal data were motor-vehicle bureaus, credit bureaus, educational institutions, law-enforcement agencies, social welfare agencies, employment agencies, health services, and regulatory agencies.

The four organizations most frequently complained about with regard to disclosure of personal data included a private investigator, a hospital, a charitable institution, and the same police force as previously mentioned.

One third of respondents reported having a written policy regarding release of personal data. In 70% of cases this policy was said to apply to customer records. The rest were evenly divided between employee and subject records. Forty-four per cent of non-profit organizations responding said they had written policies regarding disclosure of personal data; only 19% of profit-seeking organizations did. Organizations in the size range of 500 to 1,000 employees were more likely (49%) to have a written disclosure policy than were very small (21%) or very large organizations (30%).

Only 9% of respondents reported taking effective disciplinary action against staff for violation of the confidentiality of personal information. The organizations most likely to take effective action were motor-vehicle bureaus, law-enforcement agencies, public utilities, credit bureaus, and health services. Non-profit institutions were nearly twice as likely to take effective action than were profit seeking organizations.

Moreover, only 21% of respondents reported that they informed the individuals about whom records were kept of the organization's policy regarding release of personal information.

Thirty-one per cent reported that different levels of access had been established to reflect different degrees of sensitivity of personal data on file.

Forty-three per cent of respondents said that the subject of a record had the right to examine all data in it. Others placed some restrictions on this privilege. The types of organizations least likely to allow an individual to examine his own record were insurance companies, social welfare agencies, law-enforcement agencies, health services, employment agencies, and oil companies. The organizations most likely to receive complaints regarding the inability of an individual to examine his own record included law-enforcement agencies, credit bureaus, health services, regulatory agencies, social welfare agencies, public utilities, and educational institutions. The eight organizations most frequently complained about included five hospitals (one psychiatric) which received complaints principally from patients who wanted to see their record, but were not permitted to do so. The others included a board of education, a public utility, and a law firm.

The desire of hospital patients to see their records, despite institutional rules to the contrary, is at the root of many disputes. In their brief, the Ontario Medical Association said:

> Rather than a patient having the right to see any medical record concerning him, it may at times be more appropriate if he had the right to have the file audited by another person (ombudsman).

Their brief also raised questions regarding right of access to psychiatric assessments, e.g. the hypothetical situation of a person erroneously labelled schizophrenic because of misinterpretation at the data centre, then denied access to his record on the grounds that he was mentally ill.

An extract from the OMA's Report of their Committee on Applications of Computers to Medical Practice, adopted by council in May, 1971, says:

> It was felt essential that some method of access by the patient to his data should be included in any schemes of computerized medical records. The right to remove erroneous information would seem to be basic.
>
> Should an insane or severely disturbed person have access to his psychiatric records?
>
> Should a patient have the right to delete from his personal record the fact that he once had venereal disease?
>
> These and similar questions cannot be answered at this time.

In 9% of cases, the subject did not even know a record about him existed. Organizations most likely to conceal the existence of records from the individuals concerned included private investigators, law-enforcement agencies, regulatory agencies, associations, charitable institutions, credit bureaus, investment brokers, service industries, and one major industrial employer.

Only 4% of organizations which had installed computers said that installation of the computer had led to new rules regarding an individual's right to examine his own record.

ATTITUDES

The questionnaire enquired into the attitudes of organizations having files containing personal information regarding six claimed rights of the individual upon whom information was held.

1. The right to be informed of the existence of such records when they are started. All types of organizations agreed to this right except credit bureaus, which indicated strong disagreement.

2. The right to review one's personal record on demand. Insurance companies and health services voiced disagreement; police and regulatory agencies recorded strong disagreement. Other types of organizations indicated agreement.

3. The right to correct, update or rebut information contained in one's record. No disagreement was noted.

4. The right to be furnished an accounting of the uses made of one's personal record. Many types of organizations disagreed, including insurance companies, health services, merchandizing houses, oil companies, police, and major industrial employers. Credit bureaus recorded strong disagreement.

5. The right to learn the sources of personal data in the file. Insurance companies and health services recorded disagreement; police and credit bureaus noted strong disagreement. Disagreement was noted also from foreign incorporated organizations, but in our response base 19 out of 33 foreign incorporated organizations were insurance companies.

6. The right to stop the exchange of data among organizations. Nearly all respondents disagreed with this claimed right. Disagreed: banks, public utilities, health services, merchandizing houses, oil companies, investment brokers, police, service industries, and major industrial employers. Insurance companies and credit bureaus indicated strong disagreement.

An apparent paradox relative to attitudes regarding rights of subjects can be explained by a close analysis of questionnaire responses. This paradox showed up most strikingly in answer to this question which sought the attitudes of organizations to a claimed right of individuals to stop exchanges of their personalized information among organizations. On an over-all basis we found (aggregating strong agreement with agreement and strong disagreement with disagreement):

disagree	39%
agree	36%
neutral	17%
not answered	8%
	100%

which would be reported as mild disagreement with the proposition. However, upon examining the responses within each functional type of organization, we found strong disagreement voiced by credit bureaus and insurance agencies, and disagreement reported by banking and lending institutions, public utilities, general merchandizing houses, oil companies, investment services, law-enforcement agencies, and major industrial employers. Health services were split between agreement and disagreement. The service industry category was largely in disagreement with a strong minority in agreement.

Classified by legal structure, we found federal agencies, federally incorporated firms, provincially incorporated firms, and foreign incorporated firms in disagreement. Provincial agencies and municipal agencies were almost evenly split on the question. Agreement was reported by a strong majority of organizations that did not characterize themselves as to legal structure and organizations that placed themselves in the category "other".

We can identify the functional types of organizations in agreement as educational institutions, social welfare agencies, associations and organizations that did not categorize themselves as to function, with a large contribution from the health services and service industry categories. The total response of organizations primarily interested in the individual, viz: health services, associations, welfare agencies, educational institutions, and charitable institutions made up 35% of our response base. Unspecified organizations in the "not answered" or "other" categories made up another 18%.

Respondents indicated a willingness to accept two suggested regulatory provisions regarding files of personally identifiable data. No disagreement was indicated regarding imposition of standards of hardware and software provisions to ensure data security nor with establishment of standards concerned with means for acquisition and dissemination of data.

However, publishers (strong disagreement) and oil companies disagreed with the suggestion that data banks be registered, and both publishers and credit bureaus reported strong disagreement with the suggestion that periodic site inspections be made to ensure compliance with regulations.

The questionnaire also polled our sample on their attitudes regarding suggested licencing of certain personnel involved in handling personal information. Publishers as a class indicated strong disagreement with all suggested licencing, probably fearing some abridgment of freedom of the press more than interference with their handling of personally identifiable information.

Other than that, however, no disagreement was indicated to the suggestions that data-bank proprietors and information suppliers be licenced. Merchandizing houses and oil companies disagreed with the suggestion that data gatherers be licenced. Widespread disagreement was voiced to the suggestion that computer programmers be licenced. As a class, it was opposed by most federally incorporated organizations especially banking and lending institutions, oil companies, and major industrial employers. Merchandizing houses and publishers voiced strong disagreement.

The suggestion that data processing centres be licenced was opposed by merchandizing houses and oil companies in addition to the strong disagreement from publishers.

SUMMARY

This survey of 1,268 organizations employing 1/6 of the Canadian labour force disclosed that:

About half of all information operators used computers; 3/5 owned or leased the machines; the rest purchased computing services. Three fifths of computer owners had remote access facilities, 84% had at least three years experience with computers, 93% utilized large-scale machines.

Computerized records were held on at least 9 million Canadians who were regarded as customers, 8 million who were regarded as subjects, and 1/2 million employees.

The principal potential privacy invaders in terms of records held on subjects (72), recipients of personal information regarding individuals (73), and extensive use of investigators to delve into individual's lives (76), made up a small, easily identifiable group. From this point of view, the subjects of regulatory action were discernible and not too numerous to adminster effectively.

Most systems handling personally identifiable data were intraprovincial in scope. Only 8% of files were wholly or partially in the U.S. However, about half of all systems exchanged personal information with U.S. systems and in nearly all cases information systems proprietors were affiliates, branches, or subsidiaries of U.S. concerns.

Three quarters of presently computerized files were found to contain errors at the time they were converted from manual to EDP format. Three quarters of respondents said the most sensitive personal information was still in manual form.

The great preponderance of personal data was extracted from the subject himself. More data was obtained from hospitals and medical practitioners than is generally believed. Use of investigators was restricted to a few types of information systems but the technique led to most of the complaints regarding collection of personal data.

Some 342 organizations got at least some of their information about individuals from law-enforcement agencies - the supposed confidentiality of criminal records notwithstanding.

An unrestricted right of access to personal records by the individual concerned appeared to exist principally with respect to records containing relatively innocuous material. Only a minority of systems had implemented, publicized, and enforced rules to safeguard the confidentiality of sensitive personal information in files. Computerization had done little to improve this state of affairs.

Systems operators indicated a willingness to grant subjects the right to examine records and to correct and update them. There was some reluctance to granting subjects the right to be informed when records concerning them were started and greater reluctance to permit them to learn the sources of derogatory information concerning them. There was widespread opposition to granting the subjects the right to learn the uses to which personal data concerning them were put and greater opposition to according to subjects the right to enjoin exchange of personal data concerning them among information systems operators.

There was strong agreement with the suggestions that personal data banks should be registered, that standards of hardware and software security should be established, and that standards should be established regarding the acquisition and dissemination of personal data. Some opposition was reported to the suggestion that periodic site inspections be made to ensure compliance.

With the exception of some reservations arising from concern regarding freedom of the press, there was general agreement over the desirability of licencing and regulation of data processing centres and their personnel. This agreement did not, however, extend to the licencing of computer programmers.

OBSERVATIONS - U.S. STUDIES

The experience of the U.S.A. with its Federal Fair Credit Reporting Act provided guidelines but not a model by any means.

In evaluating the potential effects of this U.S. legislation, it was useful to draw upon two general observations regarding individual privacy.

The groups whose privacy was most seriously compromised appeared to occupy two opposite extremes of the socio-economic scale:

GROUP I: Upwardly mobile managerial and professional persons whose applications exceed those of the average person;

GROUP II: Manipulatable and administered persons belonging to easily identifiable groups: the young, immigrants, linguistic minorities, native peoples, the unemployed, the unemployable, the infirm, and the aged.

Returning to U.S. experience in regulation of banks of personalized data, we noted that:

1. The U.S. faced the problem of jurisdiction also, since most traffic in personal data there was (less so today) intrastate. It was after four states passed regulatory legislation, that the credit reporting industry requested federal legislation to fend off creation of a patchwork fabric of state regulation. This the Congress was able to do under its constitutional right to regulate interstate commerce -- based upon interstate affiliations among reporters and location of information recipients. Canada will have to face the constitutional question also.

2. The U.S. law is defective in several regards:

   (a) Specific exclusion is made in cases where an applicant is applying for a job paying $20,000 or more per annum, a life insurance policy with face value $50,000 or more, or a loan of $50,000 or more. Here they effectively cut off from protection of law Group I, the upwardly mobile group. Besides, in an era of inflation, dollar limits are rather tenuous things anyway.

   (b) Credit reporting agencies are allowed to charge individuals for exercising their rights regarding their record -- seeing it, etc. We have heard charges quoted from $4 to $25. Either figure

would be sufficient to deter persons in Group II -- the poor -- from exercising their rights. Furthermore, most of these people will not be able to understand their rights, let alone exercise them. One can imagine such an individual trying to explain his problem in a 100-word statement. Unless these people are accorded free access to their records and furnished professional help and advice, the law would be worse than useless -- it would by hypocritical.

(c) The law specifically exempts medical records from its provisions. Our survey showed that the medical field was second only to the subject himself as the most frequently consulted source of personal information regarding individuals.

Thus, the U.S. Fair Credit Reporting Act may well give the illusion of protection to the individual rather than the substance.

It seems essential that any Canadian policy in this regard cannot merely be imported, but must be viable within the Canadian context, and not arouse expectations that cannot be fulfilled.

TENTATIVE CONCLUSIONS

It is not our intent here to put forward detailed solutions to the problem of privacy and the computer, but rather to demonstrate that such a problem exists. However, it is impossible to escape three conclusions.

1. It is recognized that the need to know and the right to privacy co-exist and any sensible solution involves achieving a balance that is in keeping with the cultural and socio-political context of today's society. Our study showed clearly that the weight was heaviest on the need-to-know side of the scale. Some adjustment is required. Privacy has been a negative virtue and usually one has had to prove privacy was being compromised to stop some data handling practice. Perhaps, to restore balance, privacy may have to be articulated as a right and the onus put on data collectors, manipulators, and traffickers to prove that their operations do not compromise it.

2. It would seem that organizations whose principal business is collecting and disseminating personal data, especially of a potentially derogatory nature, should be subject to government regulation. In other words, Canadians should be afforded, at the least, the same degree of protection now given Americans under their Federal Fair Credit Reporting Act.

3. Finally, the government, starting with the Federal government, should first clean its own house. As a first step, massive data exchanges among departments must be controlled or at least brought under public scrutiny. Next, adequate security safeguards should be applied to government data processing and telecomputing by civilian departments. Present practices appear to be sufficiently loose as to create serious hazards. Finally, present governmental security practices need to be reviewed in their entirety. Thought should be given to development of remotely accessed secure computer systems that can automatically restrict access on a strict need-to-know basis. In this sense, modern computer technology can give us, probably for the first time since writing passed from being one of the occult arts, the facility for truly preserving the privacy and confidentiality of sensitive information.

CHAPTER 3

EMPLOYMENT

Employers gather information regarding prospective employees to aid in arriving at selection decisions. They usually continue to gather information regarding employees to monitor their performance and to make decisions regarding retention and promotion. They usually retain records of former employees to administer superannuation benefits or to arrive at decisions regarding possible re-employment. Information is gathered to facilitate the administration of employee benefit plans, although the actual administration may be carried on by labour unions, insurance companies, or independent associations such as credit unions. Employers are one of the principal sources of information about individuals. Anyone who wants to track someone down, learn the extent of his resources, or find out what sort of person he is, seems likely to call his boss.

Generally, the amount of information gathered about a prospective employee and the extent to which it is independently verified depends upon the responsibility vested in the position for which he applies. If a man wants to walk out on his wife and his mortgage, he would be better off to sign on as a transient logger or mill hand with a forest products company in Powell River, B.C. than to seek employment as a registered securities representative with a firm that is a member of the Toronto and New York Exchanges.

The Retail Council of Canada said in their brief:

> "Retailers, like other employers, obtain information from previous employers, and for particular positions, may obtain security and related information from investigation companies, credit information from credit bureaus and, with the permission of the employee, possibly health information from a variety of medical record sources. An employee who hopes to be employed in a position where his honesty, loyalty or discretion may be tested by the demands of the job, probably should expect some investigation into his record in each of these spheres."

In their brief, the Royal Bank told us that a (job) applicant undertakes to sign (as a condition of employment) the bank's Declaration of Secrecy form.

All information provided by an individual upon application for employment is considered confidential. This information is held by the bank's Personnel Department together with the data derived from performance reports prepared regularly on all employees by a reviewing director. Access to employees' record files is restricted and information from these files is used by the bank in staffing the diverse positions to be found in any major bank. These records are considered to be the "property" of the bank.

The employment application contains the following data: name; present and previous address; date of birth, height, weight, marital status, date of marriage, number of children, languages spoken and records of serious illness; preferences as to location; educational background; employment history; and names of three references.

The most searching background investigations are conducted on applicants for positions which require security clearance. These are handled by the Industrial Security Branch of the Department of Supply and Services. The applicant fills out a security questionnaire which requires positive identification of the subject including fingerprints and his complete personal history with regard to changes of name, changes of citizenship, marriage and divorce, prior employment, education, military service, changes of residence, and foreign travel. A key requirement is that no gaps be left. The applicant is also required to give names, addresses, citizenship, and occupation of his parents, immediate family, siblings, in-laws, and three to five references. Cases are assigned to the RCMP for investigation. Presumably they check their own file of Criminal Records and their Security and Intelligence files as well as public records such as registries of births and deaths, marriages, and divorces, citizenship court dockets or the Secretary of State's file, and military service records. They conduct field investigations which

entail interviewing former employers, teachers, neighbours, references, and family members. Results of the investigation are sent to DSS which then may or may not issue a security clearance to the employer.

The blue-collar worker is subject to less scrutiny than the man who aspires to a managerial professional position. The latter sometimes get their jobs through executive search consultants.

Often these consultants wear three hats: executive search, that is, a high-class employment agency where the employer pays the fee; career development which helps aspiring executives groom themselves; and organizational development, often a euphemism for hatchet men who cut "dead wood" out of client firms.

To fill a given job, the search consultant first compiles a "long list" of 12 to 100 names made up of former unsuccessful candidates still on file, career development hopefuls, job hunters who reply to advertisements, and industry contracts -- sometimes candidates previously placed elsewhere, provided a 6-month period has elapsed. Commonly, promising applicants are winnowed out by a seven-stage screening process. First candidates get a socio-emotional interview to detect severe emotional difficulties, then a Technical Interview to see if they are professionally qualified, then an IQ test. For those who remain, telephone verification,

often tape recorded, is made of former employers, educators and references. Then comes a highly personal psychological test, an investigation by a credit reporting agency to insure the candidate's conformity to the norms of a middle-class life style, and a medical examination.

Other prospective employees, not necessarily of executive calibre, are routinely subjected to investigative credit reports. These include employees of public utilities, computer firms, securities salesmen and insurance agents. Banks and hospitals have their own network for exchanging information regarding former employees seeking re-employment within the same industry. Telephone companies sometimes make such investigations using their own security force.

With reference to personnel reporting, Retail Credit of Canada stated that the proportion of rejected applications was 7.7%.

In defence of their practice of using anonymous informants to develop derogatory information regarding job applicants as well as applicants for insurance and credit, Retail Canada of Canada stated:

> "Turning to the relatively small number of persons about whom clearly unfavourable information is now developed, the result (of revealing sources of information) would be that these persons would to the extent that they obtained

benefits which they are now denied, do so at the expense of a great majority of decent and hard working people who honour their commitments and conduct themselves as good citizens."

The brief went on to state:

"Persons who work in and know the reporting industry are impressed with the rapid increase in the amount of information developed during their investigations concerning the activities of organized criminals trying to penetrate legitimate business."

This information, if credible, should most certainly be brought to the attention of responsible officials.

Regarding blue collar workers, one manager told us: "We just collect enough data on those fellows to pay them." This is generally true, unless the applicant is going to drive company vehicles, then he may be asked to release to the prospective employer a transcript of his motor vehicle driving record.

After employment, the dichotomy persists. Only executives are commonly subjected to periodic performance appraisals and compulsory medical examinations.

Most employees of all kinds have the right to see and rebut their records, although an aspiring executive might find his curiosity taken as a sign of disloyalty. Many public servants are furnished annually with transcripts. However, at least one board of education denies this right to teachers.

Among blue-collar workers, it's not what is on the record that hurts but sometimes what is not -- like disciplinary action notices and accident reports tucked away in the foreman's desk. A steelworkers union official told one of our investigators: "Our guy has a clean record so we go to arbitration, then these fellows pull out all their little slips of paper and kill us."

The Public Service Commission maintains an on-line-computerized skills inventory known as Data Stream. Basic input is the Personnel Action Form completed by candidates for appointment, this is supplemented by the Data Stream Questionnaire sent to incumbent employees. The computerized system can be accessed from 32 terminals located in government departments from coast to coast. Access is controlled by user identification and password but no audit log is kept on who obtains what information for what purposes. A number of public servants have expressed a desire to know just how much fishing goes on in Data Stream.

Employers have a statutory requirement to withhold income tax and Canada Pension Plan contributions and to report these withholdings to the employee (T-4 slips) and to District Taxation offices (T-4 supplement). When an employee is separated from employment, the Canada Unemployment Insurance Commission must confirm the circumstances of his separation to determine his eligibility for unemployment insurance benefits. The services of Retail Credit of Canada have been engaged in this connection.

Credit reporting agencies routinely seek information from employers as do prospective new employers and educational institutions. Those inquiries are usually stimulated by the employee or former employee who gives the employer's name in answer to an application questionnaire. Employers increasingly are refusing to volunteer information and often limit their co-operation to confirming or denying the facts set forth by the applicant. Insurance companies and labour unions often collect personal data from employers when insurance benefits or union membership is an integral part of the employment agreement. Where employment must be confirmed as part of an individual's application for insurance, this is usually done for the insurance company by an investigatory credit reporting agency.

Employers collect personal information about employees principally from the employee, from former employers and from educational institutions. Occasionally a prospective employee will be asked to release his educational transcript to an employer but this is most common in the academic world. Few industrial employers are prepared to evaluate properly an academic transcript.

Information may be released to police or motor vehicle bureaus but such release is generally prompted by the employee in seeking to secure some benefit such as a character reference or a bread-and-butter operator's licence in the event that his driving privileges have been suspended.

When employers require checks on prospective employees regarding past criminal involvement, these are generally made by investigative credit reporting agencies that depend upon files of newspaper clippings. The key to individual identification in such files is association of name, age, and street address of the prospective employee with those of the individual described in the newspaper story. This is the reason for requiring residence histories from employment applicants and also the reason why so many criminals today report themselves as having "no fixed address".

How employers respond to police requests for information about employees depends upon the working relationship between the firm and the police. While industrial employers generally will simply confirm the fact of employment, banks, transportation companies, public utilities, insurance companies, and certain merchants, especially jewellers, furriers, and department stores, may extend greater co-operation.

Many employers have stopped gathering information that could provide the basis of unlawful discrimination such as that dealing with race, religion, or national origin. However, one executive told us that legislation aimed at improving the status of women by granting privileges such as mandatory maternity leave is leading to subtle discrimination against them in hiring.

Many companies of any size have put their payroll files on computer and sometimes this set of computerized payroll records in fact constitutes their personnel files. More detailed personnel records on executive personnel may or may not be computerized. On-line personnel records of a detailed nature such as those in Data Stream are the exception rather than the rule. Medical records are usually kept separately, most commonly in manual form.

During the 1971 Couchiching Conference the point was raised that the RCMP had operated wiretaps in Vancouver in connection with surveillance of a break-away group within a labour union active in the forest-products industry.

At the same conference, Edward Ryan of the Ontario Law Reform Commission stated that the Hamilton Police had operated 500 wiretaps during a particular period. A representative of the Steelworkers union stated that the period in question coincided with a steel strike affecting that steel manufacturing centre. The allegation was denied by the chief of the Hamilton Police.

The use of tape recordings of employee conversations during the course of duty for disciplinary purposes came to light in a dispute between Canadian National Railways and the Canadian Brotherhood of Railway Transport and General Workers. The procedure was at first agreed to by the union for training purposes although the company was later reported to have withdrawn from the agreement and notified the union that when necessary in exceptional cases recordings would also be used for disciplinary purposes.

A radio engineer for a broadcast company told us that some years ago he was employed to make surreptitious tape recordings of negotiations in connection with a rail strike. The union would not agree to minutes being kept of the proceedings so the eaves-

dropper installed four wireless microphones in the conference room and recorded their output on an 8-track tape recorder using four different receivers as inputs. In this way, the directional properties of sound coupled with the memory of company participants could serve to identify each speaker at the bargaining table.

A repressive measure not uncommon in the States but not yet imported into Canada, at least on a measurable scale, is the internal theft ring investigation or employee bust. The investigations are carried on by a team of ex-military and police investigators who get together on an ad hoc basis when engaged as consultants. Acting upon information from undercover operatives, who had been infiltrated into the firm's employ some 6 to 18 months earlier, the group descends upon the plant. Workers are seized when passing through the gates, while on their way to their cars in the company parking lot, or when called to the office on some pretext. They are spirited away to some nearby motel where they are interrogated in relays by members of the investigative team. The interrogation often includes polygraph examination. Confessions of guilt are extracted as well as consent to searches of the employees' homes and cars.

Although the name implies that these investigations deal with pilferage or theft of the employer's goods by his employees, they have been used in cases of gambling, bookmaking, policymaking, and drug use and trafficking on the employer's premises. Charges

are seldom brought to the attention of the official police; the firm asks mainly restitution and in some cases the right to discharge the offenders without recourse to arbitration. Such procedures have been used, it was claimed, to impeach unusually militant local union leaders. The confessions extracted and goods or contraband seized remain, of course, on file and could be used to guarantee good behaviour and passive acquiesence on the part of the offenders who do not lose their jobs as a consequence of offences brought to light in the investigation.

Another unique American development that could happen here is the formation of a group of 25 recently retired senior investigators from police and intelligence agencies who work now as private consultants. One of these men, a former FBI official, told one of our investigators "We're good because we know where the files are and how to get into them." Presumably this feat requires some collusion with former colleagues still in the public service -- the invisible college works even in superannuation.

The group screens employees and potential business partners for possible past criminal or subversive associations; it screens political appointees to make sure there are no skeletons in their closets that the opposition party could uncover to embarrass the government; and it has supplied substantiating facts to a mass-circulation pictorial magazine which has gained attention for its exposé articles.

CHAPTER 4

CREDIT

We are living in a credit economy. Whether this is good or bad and the nature of its economic implications are beyond the scope of this discussion. Rather, we are concerned with the collection of personal information on potential debtors, which creditors utilize in an effort to cut their losses from delinquency and fraud.

There are three reasons why a debtor will default on a loan: he can't pay it back; he doesn't want to; or he has too many senior obligations. How the credit grantor protects himself against these eventualities depends upon the type of credit sought and the type of lending institution.

Some lenders make decisions regarding loan eligibility within their own organization but most use the services of some outside agency. These outside agencies include: 1) mercantile credit reporting agencies, 2) investigative credit reporting agencies, 3) in-file credit reporting agencies, 4) central registries of indebtedness, and 5) credit-card monitoring services. Each type of agency has unique characteristics but functions tend to overlap. A newspaper clipping service, for example, is an essential component of mercantile and investigative credit reporting but file-based

reporting agencies also keep some clippings. Clippings are gathered relating to bankruptcies, crime, accidents, non-responsibility advertisements, divorce petitions etc.

A mercantile credit reporting service deals primarily with businessmen although it may also rate individuals such as celebraties or sports figures. Its methods involve interviewing the businessman, reviewing his account books, visiting his place of business, and querying other businessmen about him, especially his suppliers. Mercantile credit reporting agencies also rate corporate bond issues as to their financial security from the investor's point of view. Summary ratings are published in bound volumes and detailed reports are supplied on request to clients -- principally other businessmen.

All credit reporting agencies assert they are not "private detectives" but they can in fact be used in that way. One of our investigators recalled how he once used a mercantile reporting agency to investigate a man, a proprietor of a business, who was threatening to sue a magazine our investigator was then employed by for libel. Generally, mercantile reporting agencies keep their files in manual form and operate within limited areas achieving nationwide and international coverage by exchange of information among branches. Their investigators tend to have accounting background and turnover of personnel is not a major factor.

Investigative credit reporting agencies deal primarily with individuals rather than companies. They investigate applicants for life, fire, and auto casualty insurance; candidates for employment; individuals seeking credit especially in the form of mortgages or travel - and - entertainment cards; and insurance claimants. Their principal sources of information are the neighbours of the subject. They probe to find evidence of excessive drinking, juvenile or irresponsible driving, wild parties, family brawls, negligent property maintenance, and obvious physical or mental impairment. Investigators also call upon the subjects' employers and, in over half the cases, talk to the subject himself. Investigative credit reporting agencies will tell you they too are not "private detectives". However, in some instances a law firm that is already a customer of an investigative credit reporting agency has been known to request a report on a prospective litigant in, say, a divorce action, although not advising the agency of the reason for the request.

The relationships of investigative reporting agencies with the police are sometimes a matter of concern to the public; we were able to establish that they, in fact, work for government agencies, investigating potential fraud cases and have, on occasion, been able to come up with a very authentic looking transcript of a subject's criminal record. Like mercantile reporting agencies, they keep their files in manual form and conduct their operations on a local area basis exchanging information among branches on a

national or international scale as circumstances dictate. Their investigators have no specific background and turnover tends to be higher than in mercantile reporting agencies. The various firms in the field tend to develop certain expertise: one excells in investigating life insurance applicants and claims -- has some highly trained investigators experienced in uncovering potential cases of fraud such as when an individual had just received the medical verdict of terminal disease and then seeks to purchase a million dollars worth of life insurance while fraudulently concealing his medical history; another agency specializes in fire and casualty work. Services are sold on a per case basis ($5) or on an hourly basis ($10) for major investigations.

A brief filed with the Task Force by the Retail Credit Company of Canada Ltd., a leading investigative credit reporting agency, put forward the proposition that there is absolutely no need for legislative control of information brokers such as themselves. It was argued that accuracy and fair reporting are almost always achieved because it is in the interest of the industry to promote this end. It was also argued that regulation would interfere with the best interests of "good citizens" and good consumers who comprise the bulk of the Retail Credit Company of Canada subjects.

It was suggested that the "need to know" by the customers of Retail Credit include such topics as the mental and physical health of the subject, and this "need to know" cannot be completely appreciated by government regulators.

The in-file credit reporting agency uses investigators only infrequently. Customarily, it gathers information for the subject's docket by contributions from the merchants who make up clientele. Information collected is largely factual in nature; it has to do with credit limits, paying habits and defaults. A charge is made to belong to the local credit association and an additional charge is assessed based upon extent of usage. Cost-per-subject-evaluated is a fraction of that incurred using investigative reporting agencies. Records are held in the form of jackets in manual files. Clerks at the local credit bureau respond to telephone queries from clients. The clients must identify themselves by a code number. These calls are usually initiated at the credit offices of merchants who belong to the association. Some file-based credit bureaus in the U.S. have become computerized and their Canadian affiliates may soon follow suit.

Credit Data, a U.S. computerized credit information agency with nationwide operations headquartered in Redondo Beach, California, told us that its Canadian files are not identified as to nationality, only that the consumer has a Canadian address. Data is supplied only

when U.S. credit grantors transact business with Canadian residents; Canadian credit grantors are not subscribers to the service. Anyone, including foreign residents, may review, rebut, and, when verified as inaccurate, have data corrected.

File information is released only to bona fide credit grantors and certain governmental agencies only as an aid in evaluating credit worthiness and for certain other legitimate business purposes. The subject is not notified when information is released to a thirty party.

All information is computerized and accessible from remote terminals. Remote terminals are located in San Diego, Los Angeles, San Francisco, Oakland, and Sacramento, California; Chicago, Illinois; Detroit, Michigan; and Buffalo, Niagara Falls, Syracuse, and New York, New York. There are no terminals in Canada. Data may also be obtained by subscribers by mail and telephone.

Nearly all credit reporting agencies in Canada are subsidiaries or affiliates of U.S. organizations. As such, Canadian consumers get some derivative benefit from the U.S. Federal Fair Credit Act if only because the U.S. firms and their Canadian counterparts find it convenient to standardize on common operating procedures. There is now a measure of forgiveness -- information on bankruptcy is deleted after 14 years; crime after 7 years; accidents after 3 years. Subjects generally may now discuss the

contents of their files with branch managers of reporting agencies and rebut unfavourable comments. Some rights accorded U.S. citizens are, however, denied to Canadians. These include the right to be informed when an unfavourable report is circulated.

A typical in-file (file-based) credit reporting office contains several power-driven elevator tub files filled with records called dockets. The dockets are small manilla envelopes that hold clippings or other pertinent documents and have additional information recorded on the outside. They are filed in order of subject's name. The recorded information includes basic identifiers: name, name of spouse, cross reference if any, address, employer, former address, and date of birth. It contains ledger entries contributed by the credit offices of member firms. These include: code number of the firm supplying the line entry, the firm's account number, date account was opened, date of last sale when the entry was contributed, high credit extended, amount owing, amount past due, terms, manner of payment and revisions if any. Manner of payment is the key entry. It is coded: 0 means an open 30 day charge account; R$XX is a revolving account with monthly payments in the amount of $XX; and I$XX is an installment account with monthly payment indicated. These notations are followed by a number, zero if too new to rate, 1 if the account is top notch, all the way to 9 for a bankrupt, each successive value connoting an increasingly unsatisfactory level of experience with the account. The jackets also contain notations of inquiries made to the bureau: date, member number, and type of inquiry.

Most people who get into difficulties with credit grantors do so by being unable or unwilling to meet their obligations. Cases where deserving persons experience difficulties tend to follow certain patterns. First, there is the wrong name syndrome. A deserving person shares the same name as a chronic defaulter. The problem can usually be cleared up by a brief visit to the local credit office and such visits are such appreciated both by the credit bureau and its member firms.

Next is the slow pay problem. Sometimes consumers unwittingly bring trouble of this kind on themselves. One individual told us he regularly withheld payment on his installment account with a storm window supplier because their first collection letter contained a stamped, self-addressed envelope for his payment and it was more convenient to use this envelope than to address and stamp one on his own. Such an individual risks having a 1 credit rating reduced to a 2 or 3 for little tangible return. A preferable course of action would have been to recognize that businessmen need their money promptly, then sort things out with the credit office of the business firm and ask the office to submit a ledger line entry revision to the credit bureau.

The most troublesome cases are bound up in the factored account syndrome. A consumer buys merchandise on time, finds it to be defective and withholds payment to force the merchant to repair or replace it. Meanwhile the merchant sells the account to a third party. Now this third party is neither a malefactor nor a benefactor. He is just an accounts-receivable factor; he wants his money and could care less if the washing machine makes a funny noise. When the money is not forthcoming the consumer's credit rating may suffer. The consumer's best strategy is to file an explanation with the local credit bureau manager and take up his complaint against the merchant with the nearest Better Business Bureau or branch office of the federal Department of Consumer and Corporate Affairs. His credit rating should not suffer unless everything he buys turns out to be "defective", which would tend to indicate that his claims were merely excuses to evade responsibility. He may eventually be forced to pay but these things tend to follow a pattern -- all the complaints we learned about, from having been filed with a consumer protection group in one Canadian city, came from one store, which also indulged in various crafty business practices: loss leaders, bait advertising and high-pressure selling. Such a merchant will soon find his own credit rating and general repute suffering as a result of disputes with consumers.

A central registry or exchange is not unlike the file-based credit bureau but is more specialized. On the provincial level some attorneys-general have established computer-based personal property security registration systems; these systems exist primarily to prevent the fraudulent sale of property subject to liens without first discharging them. The systems keep track of conditional sales contracts over $300, chattel mortgages, and assignment of book debts by companies. Most entries concern people buying cars on time. Access is free to all at $2 an entry.

Small loan companies maintain a lenders exchange through the Canadian Consumer Loan Association. This lender's exchange keeps records on debtors to see that they do not go over their credit limit (usually set at $5,000) by seeking loans from several lending companies, the exchange also holds the names of debtors who have defaulted to finance companies. A loan cannot be made to an applicant with loans outstanding from three finance companies under penalty of fine by the association. Similar organizitions exist in the hotel trade to identify "skippers".

In the U.S., ITT Data Services, a division of International Telephone and Telegraph Corp., headquartered in Paramus, New Jersey, operates a system called ACTION (Advanced Computerized Terminal Integrated On-Line Network)for subscribers whose business is furnishing loans to customers; it provides loan accounting and

management reports. Although there are currently no Canadian subscribers a feasibility study for the Traders Group in Toronto was being conducted at the time ITT Data Services filed their brief to the Task Force.

Records include: borrower's name and address, spouse's name, year of birth, amount of loan, payment schedule, outstanding balance, and delinquency status and loan charges such as rate of interest and insurance fee.

Although the system is accessed by remote terminal, each terminal points only to the specific records of the subscriber's finance office serviced by the terminal. The automated file does not contain nor disseminate credit information as such although a high-credit limit code, which indicates the limit of credit that will be extended by the subscriber, is entered and used by the subscriber's finance office.

Management reports prepared by the system only infrequently carry names of individual borrowers and less frequently carry the personal profile information contained in the record. A receipt for payment showing amount paid, allocations to interest and principal and the current balance is prepared for delivery to the borrower.

The Credit Index is a data bank of derogatory information on 9 million people who collectively have defaulted on half a billion dollars of debt. It is located in Morristown, New Jersey and is accessed by Teletype -- cost: 1/2 cent per inquiry. The file includes 13,009 items bearing Canadian addresses and deals with approximately 8,500 persons.

Credit card security services are a new factor in credit surveillance. They depend for their operation upon the computer. In the case of bank credit cards (Chargex) a comprehensive organization under the aegis of one of the chartered banks (The Royal Bank) handles the Canadian operations of an international credit card system (Bankamericard). It maintains, by computer, a running balance of charges vs. payments for every account. Each account has a debt ceiling, say $300, $500, or $1,000 depending upon the reliability the customer has demonstrated in the past. This file of customer records is updated daily to show current balance owing, credit ceiling, and any notation of trouble such as theft or loss of a credit card. Computer printouts may be distributed to information centres or a central data base can be accessed by remote video terminals. If a purchase exceeds the floor, say $50, the merchant must call for authorization to make the sale on credit. The operator checks the list and, if the sale is all right, issues an authorization number which the merchant requires to authenticate any sales draft in

an amount over the floor limit. To warn merchants of stolen credit cards whose possessors are wise enough to keep their purchases to $49.95, the credit card company issues "hot card" lists and pays a bounty, usually $25, for hot cards picked up.

In the oil company credit card field, data service organizations do not participate in accounting operations. They depend upon the oil companies to furnish numbers of delinquent, lost or stolen cards (National Data Corp.). Otherwise, the procedure is similar except the floor limit is usually $15. There are usually no ceiling differentials, just a code indicating the action to be taken.

National Data Corporation of Atlanta, Georgia told us that its files do not specify which of the names in it files are Canadian. The files contain the account numbers of credit cards which have been issued, some to Canadians. The files are aggregated by participating companies, e.g. Gulf Oil. The data include a coded response entered by the card issuers which will generate certain instructions to a person calling NDC to ascertain whether or not the card issuer wishes him to honour the card.

The company (NDC) does not know whether or not the card issuer has informed the card holder that his account is in the NDC file.

Information is released to individuals designated for access to NDC file by the card issuer.

If the card holder were to learn that some caller has been given a directed response by NDC, this information would have to come from the card issuer.

The information is in a computer file accessible from remote terminals located in Toronto, Ontario; Camden, New Jersey; Chicago, Illinois; Reno, Nevada; and Atlanta, Georgia. These centres are queried by telephone with an operator having access to the files through a remote terminal.

Types of credit include mortgages, chattel mortgages, small loans, bank cards, travel and entertainment cards, oil company credit cards, and department store charge accounts.

Types of lenders include chartered banks, near banks (savings and loan associations, credit unions), trust companies, finance companies, various credit card plans, public utilities, and merchants extending credit.

Banks extend loans in the form of mortgages, chattel mortgages, demand loans, and participate in bank charge card plans. Generally, the bank relies upon the branch manager to make lending decisions with information exchanged regularly on a manager-to-manager

basis throughout the banking community. Banks also rely upon their own records of experience with particular customers; most of their business is repeat. In the case of bank credit cards and sometimes in other cases, checks may be made with local credit bureaus on applicants who do not come to the plan recommended by a branch manager.

The principal data systems used by banks relate to demand deposit accounting. Banks are heavy users of computers and are moving towards on-line banking at tellers windows. In most arrangements for on-line banking, there is a two-key system requiring intervention of a supervisor before any customer data beyond the current demand-account balance can be retrieved.

According to their brief to the Task Force, the Canadian Bankers' Association is concerned that more attention be paid to the legitimate need of some organizations such as banks to collect data pertaining to individuals as well as the latter's consistent practice of protecting the confidentiality of their customers' data with the following four qualifications:

1) disclosure under compulsion of law;
2) where there is a duty to the public;
3) when the interest of the bank requires disclosure, e.g. the disclosure of the state of the account when suing a guarantor; and
4) with the express or implied consent of the customer, e.g. banking references given at the request and with the knowledge of the disclosing bank's customer.

The Canadian chartered bank falls under the class of organizations which do not collect and sell information as their main business and hence should not be subject to adhering to an exhaustive list of required disclosures of practices before any possible data bank regulatory authority. The Association pointed out, "Little or no heed has been paid to the fact that banks in Canada have maintained with integrity and discretion for over a century what are probably some of the largest banks in the country."

In a detailed and highly informative brief the Royal Bank of Canada told the Task Force:

> "When a person applies to a bank for a loan he gives up a certain amount of privacy in providing the basic personal data and financial history which is required to provide a full assessment of his credit-worthiness. Any information provided by the customer to a bank is considered as 'privileged' between bank and customer. (It) is considered as the 'property' of the customer."

In the case of a borrowing client who is not well known to the bank, a credit report from his previous banker or a commercial credit bureau will be obtained. Information furnished by a referee or an outside agency to a bank is considered to be a confidential disclosure to the bank and is treated as such. It is considered as the "property" of the bank.

In conducting the affairs of any customer, a bank will build an opinion as to customer's character and credit-worthiness. These opinions are considered to be the "property" of the bank. A bank will provide upon request an "opinion or reference" on a customer under specific conditions.

(a) By request of the customer. In practice the customer's authorization is obtained before releasing details of account balance, security holdings, loans, etc.

(b) Under provisions of a statute.

The Bank Act gives the Inspector General of Banks the right of access to the affairs of a bank and annually requests the submission of certain information regarding loan accounts. The Act also covers unclaimed balances where deposits unused or unclaimed for 10 years are forwarded to the Bank of Canada with full particulars.

The Income Tax Act requires the reporting of income earned or income payments by way of ownership certificates and the annual T-5 return. A bank is also required to comply with "Requirements for Information and Production of Documents" when received. The customer is notified of any information furnished to the Taxation Director.

Other agencies also have investigative powers: estate investigations, Department of Veteran's Affairs, Welfare Agencies, Indian Affairs, Securities Commissions, and the Department of National Revenue. Where the customer has not authorized release of the requested information, a bank will notify a customer of the information provided.

(c) Process of law.

This covers orders for information such as a subpoena, summons, search warrant or other order; written notice to the customer is automatic. A bank is also liable for seizure of customer assets under Writs of Execution, Garnishment, and Judgment. In Quebec, upon receipt of notice that a depositor has sought protection under the Lacombe Law, banks file a composite claim with the court.

(d) In the course of normal bank/customer commercial operations.

These include convenience or courtesy disclosures such as new account references when a customer is moving to another branch, Letters of Information, Informal Letters of Credit, and rectification of errors.

A bank will provide to a Credit Bureau, upon request, a credit reference with regard to personal installment loans not secured by liquid security or government guarantees. The report covers the following areas only, with the name of the reporting branch not revealed.

1) Length of experience

2) Maximum credit

3) Payment experience

4) Confirmation of existing loan position.

Certain firms are permitted to enquire directly from the branches receiving a brief credit report omitting amounts of borrowings or deposit balances.

Upon request a written credit reference on an individual will be forwarded to another bank. Informal reports encompass all requests for credit information taken by telephone or across the counter. The majority of cases refer to queries regarding cheques to be negotiated or certified.

Near-banks are perceived as following the lead of chartered banks in their lending practices, and in the computerization of demand deposit accounting.

Trust companies generally require investigative credit reports on mortgage loans, their biggest lending activity. They are also moving towards computerization and on-line operation of customer accounts.

Finance companies rely upon the lenders exchange and on personal investigation by their branch managers for small loans. Some finance companies are going into the mortgage business but

are still trying to operate with the same investigative procedures that they have traditionally used in the small loan business. An official of a lending company told us that two of his competitors, both subsidiaries of U.S. companies as was the company furnishing information, were preparing to institute on-line lending operations which would function with the aid of U.S. based data files. With the exception of these two companies, most loan companies batch process customers loan records at their Canadian headquarters. This is done primarily to audit financial transactions of their branch offices. In some branch offices, access to customer files is a casual affair with minimal data-security measures in effect.

Travel-and-entertainment card activity based in Canada is limited to major transportation companies. They use investigative credit reporting agencies to check on applicants. Hot card lists are exchanged regularly among transportation companies.

During our site visit to Air Canada, we learned that air passenger manifests are kept six months and regularly consulted by local police and the RCMP.

Four travel-and-entertainment card companies filed written responses with the Task Force. With regard to the number of Canadian names on file: American Airlines of Lake Success, New York, said they had 1500; the Diners Club, 75,000; Carte Blanche of Los Angeles, California, 14,271; and American Express of New York City, 130,000.

American Airlines obtains an in-file report supplied by a local credit bureau in Canada before issuing a card. They look for adverse information such as non-payment of bills and lawsuits. If an applicant is turned down he is told whether the action arises from Credit Bureau information or company policy. Customer address information is kept in a computerized system. In the case of seriously delinquent accounts, privileges are cancelled and the balance turned over to a local collection agency.

Diners Club maintains its master cardholder file on computer and its cardholder application file in manual form. Rejected applications are filed separately for a period of two years. Information is released to Diners Club associates and to collection agencies and attorneys used for collection. Cardholders are informed if an account is referred for collection. The computer is located in Denver, Colorado. Remote access terminals are located in New York, New York; Miami, Florida; Los Angeles, California; and Denver, Colorado. Canadian associates of Diners Club must use mail or telephone for inquiries.

Carte Blanche maintains its member master file, alphabetical listing file, and list rental file on computer. The membership application file is kept in manual form. Information is released to other credit grantors if Carte Blanche is named as a reference by the member. Write-off information (uncollectable accounts) is supplied to credit bureaus Members are not notified when information is released to third parties. There is no remote access to computer files.

American Express says that their Canadian cardholer files carry a special identifying number. Information is released when a cardholder gives American Express as a credit reference or when such information is subpoened by court order. In the latter case, the cardholder is not notified. The computer is located in Phoenix, Arizona. Remote access terminals are located in New York, New York; Miami, Florida; and Phoenix, Arizona. Merchants may call the New York centre for authorization in the case of certain purchases. In all, American Express services 3 1/2 million cardholders. The integrity of remote-access terminals is ensured by the use of passwords, identifying codes, procedures which limit access, and the presence of on-site security agents.

Transportation companies are, of course, major users of on-line remotely accessed computer systems, principally for passenger reservations. Oil companies are major users of computers in processing customer accounts receivable as well as other business files. Applicants for oil company credit cards are checked out by mercantile reporting agencies (commercial users) and investigative and file-based reporting agencies (individual cardholders). There is a perceived trend away from use of investigative reporting agencies and towards use of file-based agencies. Use of computer-based credit card-service agencies is seen as an accelerating trend.

Mercantile credit cards are really just an extension of merchant's traditional credit granting practices. Computer operations are important to large department stores for processing their receivables. There is a perceived trend towards centralization in multi-outlet chains. Heavy reliance is placed upon file-type credit reporting agencies. Applications for credit are usually painless and informal, and verification usually consists of a simple telephone check with the local credit bureau.

In their brief to the Task Force, the Retail Council of Canada said:

> "For a variety of reasons, credit experience may (also) be exchanged directly among credit grantors . . . . In the cases of the more informal exchange of information, formal assurances of confidentiality have probably not been established."

During our site visit to a Quebec City department store, we learned that lists of shoplifters are maintained and regularly exchanged among stores.

Credit reporting agencies, especially of the investigative type, have branched into several collateral services. Retail Credit of Canada has established or taken over in-file credit bureaus serving several defined metropolitan areas. In the U.S., Retail Credit has set up computerized file-based operations on a

regional scale. Other ventures by investigative credit reporting agencies include insurance claims investigation, central registries of insurance claimants or high-risk individuals who might apply for certain types of insurance, property value appraisals, management consulting, and market research and consumer opinion polling. These services have in common the gathering, collating, and, frequently, disseminating of sensitive information concerning individuals.

The Task Force obtained its information on market research operations in Canada from one of its consultants who is professionally active in the market research field and who confirmed her submissions in informal interviews with her professional associates. No market research organizations were scheduled for site interviews.

Market research in Canada is generally bought and used by clients -- manufacturers or service organizations. The market research house generally carries out the actual research operations. An advertising agency sometimes commissions its own research but generally acts as a middleman between client and research house.

There are several commonly used methods of conducting market research. These include: once-only mail questionnaire, regular mail consumer panel, personal telephone interview, personal door-to-door interview, and in-depth group interview.

In all these methods, there is a contact by mail, telephone or in person with an individual respondent; a questionnaire is completed and all questionnaires are collected at a central point; all questionnaires are tabulated and aggregate information prepared; the original completed questionnaires are stored for about 6 months; and aggregate information is transmitted to the client.

Because virtually every topic from soap purchase to sex habits is investigated through market research, the position of the respondent and the handling of individually identifiable responses are of central interest. In all cases, the respondent has the option of non-response to any or all questions. In general, however, no attempt is made to explain to a potential respondent the ultimate use to be made of the information gathered or the actual impact of the questions asked. In fact, the interviewer himself may be unaware of the implications of the study. Unless all co-operation is refused the respondent has little control over what might be perceived subsequently as undesirable use of personal information.

From the time information is taken from the respondent until it is put into aggregated form and the original questionnaires destroyed, it can be lost, stolen, or mis-used. The fact that the market researcher may have collateral interests can increase this danger.

Organizations in the market research field have done a lot to improve their techniques and they generally recognize the value of research results and the need to protect them. However, this concern for security is for the benefit of the client, not the respondent. No clear evidence exists that action has been taken to safeguard the rights of respondents.

Somewhat allied to market research studies is the mailing-list issue.

Traffic in names is a very real commercial proposition. A college friend of one of our team members worked his way through school by gathering up student directories from all over North America and selling names in them for 3¢ a name. As another example, the going rate of motor vehicle registrant lists has been 1¢ a name. The action of Manitoba in raising its price per name to 10¢ poses a dilemma to mailing list suppliers serving the automobile industry. If they pay 10¢ a name to Manitoba, all other provinces and states are likely to raise their prices also, which would take much if not all the profit out of the mailing list business. If they do not pay, they will have to begin issuing mailing lists and compiling statistics for North America less Manitoba.

Business magazine publishers have refined and cross classified their mailing lists as a result additional subscriber data gathered by offering specialized publications, conducting mail-out reader interest studies, using ballot-check columns on subscription renewal forms, and compiling lists from reader service requests ("bingo" cards) and other reader inquiries. These lists are rented for one time use only to commercial organizations (user never gets to see the list, all he buys is mailing service) for rather substantial sums. Professional associations have adopted similar tactics with regard to their membership lists. The Institute of Electrical and Electronics Engineers (8,485 Canadian members) told us that they limit such dissemination to educational opportunities.

Most mailing lists today are derived from input documents which permit the subject to indicate whether or not he wishes to receive mailings. This is a partial solution to the dilemma in respect of direct mail advertising as an invasion of privacy: roughly, half the population regards "junk mail" as an essential information input, the other half hates it. Direct mail does lead to some unfortunate consequences. A young mother-to-be got on a mailing list as the result of pre-natal medical services she had received. The mailing list was subsequently sold to a chartered bank. The woman lost the baby by miscarriage and suffered further mental and emotional trauma upon receiving an eloquent congratulatory note from the bank at about the time her child would have been born.

Obscene literature and solicitations received in the mail -- sometimes in "plain brown wrappings", sometimes unfortunately not -- are sent out over mailing lists derived from a wide variety of improbable sources. One victim got listed by ordering a book on horse breeding from a clearing-house operation.

In the U.S., there is a rather effective check on this sort of thing. A person who does not wish to receive obscene materials can list his name with the U.S. Postal Service. It then becomes an offence to send obscene literature to him, or to anyone on the list. It is incumbent upon the mailer to check his mailing list against the current copy of the Postal Service's interdicted list before mailing any obscene materials. The interdicted list is available periodically in machine sensible form from the U.S. Postal Service at rather substantial cost to the user.

Many mailing lists are compiled from open sources. A good many shut-ins who could not otherwise be gainfully employed earn money clipping announcements of executive promotions, engagements, weddings, births and deaths from local newspapers. These are sold to various merchants including caterers, cake bakers, travel agencies, shoe bronzers, and tombstone salesmen.

The magazine publishing business gives rise to another problem. In this highly competitive arena, a publication hates to lose a subscriber. If a subscriber fails to renew his subscription, most publications will make a determined effort to regain him as a subscriber. Generally a computerized routine is triggered by a subscriber's failure to renew. First of all, he continues to get the magazine for some four months or so and his name continues to be reported to the Audit Bureau of Circulations as a satisfied subscriber in good standing. It is its reports to ABC that the magazine uses to justify the rates it in turn charges advertisers. The subscriber meanwhile gets a series of letters ranging progressively from gentle reminders at the expiration of his subscription to offers of various gimmicks, such as free books. In some cases, he may receive a bill for the four months additional service he got without asking for it. This bill may be followed by a collection letter. A publisher one of our staff once worked for had set up a wholly fictitious organization that sounded as if it were an international black list; its address was the back door of the publisher's home office. Letters from this ectoplasmic organization pointedly reminded the subscriber of his moral obligation to pay his bills and alluded to dreadful consequences if he did not do so. Of course, nothing unpleasant ever really happened to the recalcitrant subscriber and in due course he ceased to receive the unwanted publication. Nevertheless, the data collected upon him

could have been used to prepare a black-list, and at the very least may have created anxiety in the minds of some persons who had, in fact, not incurred an obligation let alone reneged on it.

Many unpleasantries between merchant and customer which result in credit controversies have arisen over unordered merchandise received in the mail. Such problems have been greatly reduced since one province took the bold step of relieving the customer of all obligation to pay for such material.

Closely allied to the practice of sending unordered goods in the mail is the operation of some book clubs wherein the current selection is sent to the member if he fails to fill out a rejection form and post it before a certain date. Frequently the date of receipt by the customer of the rejection form and the date by which it must be mailed are so close together that the customer has really no option to decline an unwanted selection. If he subsequently receives the book in the mail and returns it or refuses the shipment there is no guarantee that he will not be billed for it anyway; and if he doesn't pay, neither is there any guarantee that his failure to do so will not, despite a letter of explanation, trigger a computer-based collection campaign.

Readers also come in for trouble with credit agencies if they happen to be delinquent borrowers at public libraries. In Edmonton, overdue accounts valued at $14,800 were turned over to a collection agency which makes the borrower's name available for credit checking and could result in a lowering of the offender's credit rating. The first overdue notice is sent out 14 days after the book becomes due. A series of three notices is sent by the library. Five weeks later, the account goes to the collection agency.

Readers who avail themselves of public library services were subjected to certain invasions of privacy in the U.S. by federal officers who were apparently searching for readers whose reading interests lay in the Boolean intersection of the subjects: Marxism and the chemistry of explosives. The officials were looking for the perpetrators of terrorist bombings but in the course of the investigations some innocent persons with weird reading tastes came under unwarranted suspicion. Automated circulation systems that exist in some libraries make possible compilation of reading tastes of patrons; this capability, apparently little used or appreciated in Canada, could have sinister potential for political surveillance if misused.

CHAPTER 5

WELFARE

This nation has made a commitment to furnish the basic essentials of life to its citizens if they are unable to purchase them from their own resources. These essentials are perceived to include food, clothing, shelter, medical care, and education. The question of an applicant's ability to pay is crucial in deciding the merits of any application for social assistance.

Means testing is pervasive in the case of student awards; there is substantial reason to believe that it is common practice for applicants and their families to understate income and resources when applying for them.

Applications for student awards are often centralized on the provincial level. The following procedure is typical of those followed by the provinces in processing student award applications. Applications are first checked by computer to see if eligibility criteria are met. Generally, income data is taken at face value in making this initial decision. A sample of the applications is pulled, sometimes 25%, and these are manually audited for reasonableness. Applications of siblings may be cross checked for consistency. Repeat applications are checked against former applications and any drop in reported income of $500 or more is flagged for investigation.

Administrators of student award plans recognize that it would be to their advantage to run the file of applications against income reported to taxation authorities but this is permissible only in the Province of Quebec.

Awards that are denied or questioned are sent to awards officers at educational institutions for investigation. The zealousness of these awards officers is highly variable. Some do a great deal of investigation. Others tend to take the student's statements on appeal at face value. Documentary evidence such as T-4 slips or copies of the T-1 returns to confirm the student's or his parent's income may be requested or balance sheets may be sought from chartered accountants in the case of fathers who are businessmen.

Some awards officers have used the computer to compare the student awards files with campus parking permit files since ownership of an automobile often means a mandatory reduction in student award. A few awards officers call upon local businessmen to verify statements regarding a student's father's income.

Students who claim to be self-supporting are often required to submit substantiating evidence in the form of marriage certificates or letters from clergymen or other reputable persons attesting to their status. We have uncovered cases where awards officers have applied pressure through the employers of fathers who

have asked children beyond the age of responsibility to leave home because of incorrigible behaviour to reassume responsibility for their support after they gained admittance to university and applied for student awards. Of course, administrators of the student awards system gather data from educational institutions to confirm that persons receiving awards are actually in attendance.

National Health and Welfare collects personal data in the administration of its supplemental Family Allowance programme. Canada Pension Plan and Family Allowance payments are not now means tested and in administering these plans National Health and Welfare merely confirms the facts of life, death and age with the lists maintained by Provincial Registrars.

Old Age Security and Guaranteed Income Supplement is means tested and applications are sent to National Revenue for verification by comparison with income tax returns.

National Health and Welfare is attempting to reach agreement with other western countries regarding the transfer of payments to old age pensioners. Such an agreement has been reached with Germany. A person living in Germany who is eligible for benefits from Canada will have his pension information transferred to the German system. Agreement will then be reached in each case on benefits due. Germany will pay the pension and bill Canada for its share.

Disability, blind and rehabilitation benefits are initiated by application at a local office. The records, which contain medical information for verification, are kept in manual form.

National Health and Welfare does not release information in individually identifiable format. Requests for RCMP or other police are refused. Appeals by individuals are initiated by application at local offices. The appeals records are handled manually at the regional level.

The department is working on a proposal for a Family Income Security Plan. If approved, it will replace both the Family Allowances and Youth Allowances Programs. It is an income based program with applicants reporting their income and verification by National Revenue Taxation on records furnished to them by National Health and Welfare. This is the same procedure as utilized with G.I.S.

Some provincial health plans offer reduction in health insurance premiums to low income subscribers. Support levels are fixed with reference to net taxable income and these data become part of the benefit recipient's computerized file. Only in Quebec is direct verification with tax records permitted; elsewhere, an applicant may be asked to produce T-4 slips in support of his statement of income.

Related to means testing is the perennial question of automobile ownership by welfare beneficiaries. Most professionally trained social workers recognize that an automobile can be a necessity for families living in remote areas, men seeking employment, or families caring for disabled or infirm members, but municipal governments often hold differing views. We have not uncovered evidence of any massive checks of welfare roles against motor vehicle registrations, although in many provinces this would indeed be possible. On the other hand, it is an easy matter to link a licence plate with its owner on an individual basis; this appears to be the means used for gathering information in such matters.

During out site visit to a municipal social services department we learned that municipal welfare consists of aid to transients, temporary benefits, and permanent benefits. Aid to transients consists usually of putting them up for not more than four nights in sexually segregated youth hostels. Minimal information is gathered regarding transient youth.

Temporary assistance may be granted in the form of money for food and shelter; day care, clothing, and medical or dental care. Temporary assistance is given subject to minimal checking but the willingness of welfare officers to extend aid depends to no small extent on the funds remaining in the municipal welfare chest; the less the money available, the tougher the welfare officers become.

Permanent beneficiaries are as follows: aged; family units with employable head or with unemployable head; and single persons employable or unemployable. Applicants visit a branch welfare office and complete an application for social allowance. Even this can be degrading; in at least one of our eastern cities they must use the rear door of city hall so as not to soil the magnificance of its centennial-project lobby. The application commonly calls for basic identifiers, last employment, last receipt of social allowance, monthly income, statement of assets, list of dependent and non-dependent members of the family, financial data on shelter, aliases used, date the applicant moved to the city and province, next of kin, religion, and service in the armed forces. The applicant must sign an affidavit attesting to the accuracy of the information.

At times welfare officers seem to play a game of musical benefits, that is, they try to push the responsibility off on some other city or province -- the place where the applicant last resided or where his parents or spouse live.

Next a case worker completes an assessment form for the applicant. This requires information on education, health, age, body size, workmen's compensation, registration for employment, job history, reasons for leaving last job, skills and professional technical qualifications, whether the applicant would relocate for employment, and financial and counselling services requested.

If an applicant is deemed to be employable, workmen's compensation and unemployment insurance are checked before assistance is granted. Canada Manpower may be checked to make sure the applicant is actually seeking employment. Enquiries may also be made as to whether the applicant is receiving or entitled to benefits from the Department of Veteran's Affairs.

A female head of household can encounter special harassment when applying for Mother's Allowance. She may be importuned to initiate legal procedings against an absent husband, or name a putative father for her child or children. In one city, about one family in ten receives a home visit in which a social worker checks for fraud and assesses the need for further service. In some instances the social worker may be looking for a live-in boy friend who can be coerced into providing support for the mother and her family.

An applicant who claims to be physically disabled must be examined by a physician, or optometrist if his disability involves blindness. These medical reports become part of his record. If the applicant is unwilling to report at the time and place specified for examination, his claim may be disallowed. The applicant has the burden of establishing that his condition renders him unable to travel and his oral protestations are seldom taken at face value.

An eligible applicant is issued a card with name, address, sometimes photograph, and signature. In one city, 30 cases of fraudulent use of welfare cards were reported in May 1971. If an application is denied, the applicant may appeal through his case worker and the case worker's supervisor, to the welfare administrator and to a Board of Review in the order -- about one fourth of the appeals are successful.

Even where welfare records have been computerized an EDP (electronic data processing) file generally contains only a subset of the total information gathered by a case worker. Typically this would be name, address, marital status, benefit classification, dependants, data, area of city, assistance received, means of payment, eligibility code, payments to hydro, and marital status of dependants -- it is principally a file to facilitate payment, given that eligibility has first been established.

Officially, police and credit agencies do not have access to welfare files but in fact there is a close working relationship. Police investigate cases of welfare fraud; in at least one city a detective has this as a full-time assignment. In return, some welfare officials may provide data on benefits received by persons in whom the police are interested. We have already seen how credit investigators are used by welfare organizations to determine the circumstances under which a welfare recipient left his last job;

it has been alleged that at least on one occasion welfare officers alerted the credit reporting agency when their beneficiaries received payments that could be used to help clear existing debt.

Medical and dental services, drugs and prosthetic appliances are supplied free of charge to welfare beneficiaries. Provincial health plan records are flagged to designate welfare cases. There can be little doubt that health service professionals are well aware when they are treating welfare recipients. They seem to be utilized more frequently in teaching and research situations than self-supporting persons. Money-saving proposals such as a cost/benefit allocation of medical resources, and establishment of disincentives to seeking benefits outside of the province seem to be applied more vigorously to welfare recipients than to self-supporting persons.

One unemployed man suffering from kidney disfunction was, in effect, told to put his affairs in order and go home to die quietly. He rebelled against this verdict and went to the United States where he sought and obtained a successful transplant operation. The provincial health plan at first refused to pay his medical bills, which lead to several acrimonious exchanges including the dunning of relatives not legally responsible for the man's care. Intervention by a member of the provincial parliament was required before the case was resolved in favour of the welfare recipient.

Disincentive to seeking medical care outside of province -- which includes women seeking abortions on demand, as well as travellers who are taken suddenly ill in another province -- often means slow pay, no pay, and short pay which is damaging to both national prestige and to the credit standing of the patients, who usually come in for more than their share of dunning letters when their public health plan defaults.

Among the most numerous welfare beneficiaries are Canada's native peoples. A particular indignity that can be inflicted on them is that of travelling sociologists who probe their personal lives in the name of research. In Inuvik, one visiting social scientist was thrown into the Mackenzie River for asking too many personal questions. Other Canadians come in for similar study on occasions. A Youth Survey conducted by the Department of National Health and Welfare in the summer of 1971 asked teen-age girls why they didn't wear bras and what this told about thier personality, character, and habits. The survey, which dealt with issues such as use of drugs and sexual behaviour, as well as bras for teenagers, came under the cognizance of the Fitness and Amateur Sport Division. The Division is one principal research branch of National Health and Welfare; it also keeps information on the Fitness Awards Programme, and the resources and personnel in the programme.

The Department of National Health and Welfare is developing a health data service for the Northwest Territories. A service bureau would be maintained in Ottawa linked by the two-way terminals in a telecommunications network. The health records of 35,000 individuals would be incorporated in this system and would contain information about doctors, facilities and social factors such as alcoholism. These records would be accessed by terminals in health offices and hospitals, and used to evalute the level of health in the region.

The Department has only recently begun to consider the problems of confidentiality and privacy in the design of telecomputing systems. At present, manual records are kept in regional and central offices and the level of security appears to be minimal.

Somewhat allied to social welfare agencies in their eleemosynary activities are charitable institutions. No organizations in this category were visited although 54 answered the Task Force questionnaire. The United Company Fund of Greater Toronto, however, filed a brief in the form of a short letter to the Privacy and Computers Task Force. The Fund outlined its record-keeping activities, which are computerized.

It was pointed out that its records were regarded as private information and kept confidential through the use of limited physical access and strict security arrangements with the data centre.

The fund maintains and updates records related to previous donors (about 750,000) and preprints pledge cards for use in the upcoming annual campaign. Similarly, records are kept related to the collection of pledges or payroll deduction contributions. The mailing list is not made available to other groups or organizations.

CHAPTER 6

INSURANCE

Cheating the insurance company seems to have been an international activity of at least 100 years standing judging from the extent of measures the companies take to protect themselves from inaccurate applications and fraudulent claims. Generally insurance companies find it necessary to gather and utilize a great deal of information in the processes of underwriting policies and adjudicating claims. This information is kept in manual form although essential facts may be exchanged among companies, usually through the medium of central information bureaus. Information for policy maintenance such as premium payments and contract modifications are often computerized. The industry was early to embrace the computer and its operations are frequently conducted on a large scale. Information is batch processed on a centralized basis. There has been little interest in teleprocessing although such applications are a distinct possibility for the future.

Some companies exchange information through a central reference bureau which utilizes terminals accessing a central data base. Remotely accessed computers are used in actuarial computation but no personally identifiable information is transmitted. Personalized information on file is used internally and insurance companies jealously guard it for their own commercial purposes.

Information is released to police in fraud investigations. Personnel are generally cautioned about discussing the affairs of the company or its policy holders in an extramural setting but there are as many gossipy clerks working for insurance companies as for health plans or for any other institution.

Separation of routine policy maintenance information from underwriting information by computerization of the former tends to restrict the internal dissemination of personnel data and thus contributes to confidentiality of policy holder information. Legal requirements such as reporting dividend income to National Revenue necessarily contribute to some loss of policyholder privacy.

Procedures regarding underwriting and claims investigation procedures differ in the life, casualty, fire and automobile fields.

In the life insurance field, an applicant relates information to the agent which is then forwarded to the home office. The application is subject to medical examination and inspection. Medical examination consists of the applicant giving a medical history and signing a blanket release of medical information held on him by professionals or institutions. He may also have to undergo a physical examination, the report of which becomes part of his application.

The brief submitted to the Task Force by the Canadian Life Insurance Association stated that "the life insurance companies in the collection, use and storage of 'sensitive' information are not engaged in the invasion of privacy because there is a legitimate purpose, and security and confidentiality are maintained." As evidence, the brief argued that there have been few recorded instances of an individual's suffering loss from the information gathering and using activities of an insurance company. The brief suggested that if legislation is developed in this area it should be as uniform as possible across Canada and internationally.

Much of the brief is concerned with the use of medical information by life insurance companies. They are all hooked-up to a central computerized Medical Information Bureau in the United States. The basis for such an operation and the procedures surrounding it are discussed in detail. The Canadian Life Insurance Association believes that the individual's rights to privacy are adequately protected.

In using the central computerized Medical Information Bureau a check is made by teletype with the master file in Boston, Massachusetts. The teletype dials directly into a computer index file serviced by the Recording and Statistical Division of Sperry Rand Corp. According to information furnished to the Task Force by the Medical Information Bureau, the file contains medical

information in coded form on 800,000 Canadian citizens or residents. These files are segregated according to Canadian residence from others kept by the Bureau. Individuals are listed by name, birthplace, and date of birth.

The MIB is an unincorporated membership association of 700 life insurance companies including 80 Canadian companies. Its executive offices are in Greenwich, Connecticut. The bureau's principal function is to alert insurers to hazards and impairments discovered by other insurers and not revealed by the applicant. When an insurer declines or rates an applicant because of medical treatment for a serious ailment, the coded resumé of significant information is transmitted to the bureau; action of the company is not. Occasionally reports are made to the Bureau of favourable results of medical tests that may have future health significance, and reports of favourable subsequent medical history may be communicated when there has been a prior adverse history noted in the file.

However, any type of information may be the basis of a report to the Bureau. Although 90% of reports reflects coded medical information, 10% reflects non-medical information. Code symbols used here are non-specific and merely suggest the need for special investigation of the applicant.

The Bureau receives 1-1/2 million reports for member companies annually - one Canadian company registers about 1,000 names a month. The Bureau answers 18-1/2 million requests for information each year.

The MIB information alone may not be used as a reason to decline or rate an application, but must be verified by independent investigation. This could involve checking with the company registering the case.

The Bureau feels that most applicants for life or health insurance realize that some inquiry will be made as to insurability. In most cases, a specific authorization permitting such inquiry is incorporated in the fine print of the insurance application.

The medical director (a physician) of the insurance company evaluates the applicant's self-written medical history, report of physical examination, and any information developed through the MIB check. He may also seek release of hospital or medical service records. An applicant for life insurance who is rejected on medical grounds is given no reasons for refusal. The comment that dark skin is a medical impairment can be heard among life insurance agents.

Normally the coerced consent to release of medical records poses no deep social problem since the purchase of life insurance is a private contract between insurer and insured. However, where participation in a life insurance plan is a prerequisite to employment, the question takes on a different complexion. A case came to our attention of a young man who refused to sign the blanket release of medical records. After considerable correspondence with the insurance company, an exception was made in his case. It turned out he was a highly skilled computer programmer whose services were urgently required by his prospective employer. Had he been a less well qualified individual, his bargaining power would doubtless not have prevailed and he might well have been faced with the choice of surrendering part of what he perceived to be his personal privacy or joining the ranks of the unemployed.

Applicants for life insurance are inspected by an investigatory credit reporting agency that may interview the applicant and will certainly interview his neighbours, present and former employers. The agency looks for evidence of excessive drinking, loose sexual morals, questionable associates, and involvement in criminal activities, scuba diving, sky diving, or private flying. The severity of the inspection depends upon the face value of the policy and for large policies, it may involve a detailed personal investigation by an experienced investigator for which the insurance company pays handsomely indeed.

Most life insurance companies employ staff investigators to delve into benefit claims and call upon investigative credit reporting agencies in this connection also. Of course the insurers co-operate closely with police in cases of suspected fraud, homicide, and suicide. Occasionally bereaved relatives have complained about what they perceive to be unnecessary and inconsiderate intrusion upon private grief.

Insurance companies which write policies designed to recompense policy holders in the event of illness, accident, or disability make use of the Casualty Index maintained by Hooper-Holmes which contains insurance histories of more than nine million people in the U.S.A., Canada, Puerto Rico, Central and South America. According to information supplied to the Task Force by the Hooper-Holmes Bureau Inc., the index is intended to protect insurers against frauds by present or prospective policyholders. Applicants can be checked by wire or mail -- hourly service by teletype.

Claims can be checked to learn whether other companies are on the claim, whether the policyholder has filed claims with other companies, or whether his claim history is clear. The service is said to be useful in determining whether new impairments arise during a period of contestability and to possess exclusive information regarding organized fraud rings.

Investigative credit reporting agencies also play a role in the casualty field, differing from the life field in that here they may sometimes be called upon to maintain surveillance on former policyholders after a claim is paid.

Applications for fire insurance policies are also inspected by investigative credit reporting agencies which also do claims investigation in this field, working closely with the police, fire marshall's office and the Fire Underwriters Investigation Bureau based in Montreal. Inspection of a fire insurance risk involves probing into details of the construction of the building, fire prevention features, location and effectiveness of the nearest fire department, incidence of fire or civil commotion in the area, maintenance of the property and neighbouring properties, and the general reputation and financial solvency of the owner. Such inspections are biased from square one against cabbage town and any native reserve. The FUIB maintains an index of fire claims and sends cards called LIB or Loss Information Bureau cards to correspondent insurance companies weekly so they can update their local card files and determine whether or not an applicant or claimant is too risky a prospect based upon his previous claims history. These data come primarily from police and fire marshalls. The LIB cards now contain data relating to burglary claims and other loss claims.

Burglary and theft insurance claims investigation leads to close co-operation with the police. Information from police stolen property files is made available to insurance companies as are general occurrence reports describing the crime. There is speculation that a lively international traffic in contraband takes place defrauding both insurance companies and Canada and U.S. customs. A summer settler, say imports a lawnmower, power saw, or outboard engine for his own use, reporting it to Canada Customs. He sells it to a Canadian then fraudulently reports it stolen. He obtains a police report which clears him with customs when returning to the U.S. and also provides a basis for an insurance claim against his carrier in the U.S. It is believed that a similar traffic in furs, silverware, and imported cameras may move in a southerly direction.

Insurance companies come in for a good deal of criticism with regard to automobile insurance, especially public liability and property damage. Part of the problem is that society insists on regarding operation of a motor vehicle on a public highway as a privilege and a luxury whereas it has become a necessity.

Applicants for auto insurance are inspected by investigative credit reporting agencies. Inspectors are told to find age and whereabouts of children in a family -- so the policy-holder can be required to pay more premium money as his sons reach the

age of 16 -- condition of car and its daily mileage, whether it is garaged or not, the driving reputation of the principal driver -- and if under 25 whether he is irresponsible, a show off, or has drinking habits -- employment reputation and personal-family reputation. Aged persons, military personnel, disabled persons, and drunks come in for special scrutiny. Sources of information are employers and neighbours.

Rejected applicants have the options of seeking out insurance from carriers willing to assume bad risks at what may be prohibitive cost or driving at their own peril after contributing to a provincial uninsured motorist fund.

Motor vehicle bureaus co-operate closely with auto insurance companies furnishing on demand transcripts of drivers' records giving basic personal identifiers, status of licence, prior accidents with blame indications, and all convictions for Highway Traffic Act infractions. These transcripts are useful to the insurance company not only to select among applicants for insurance but also to impeach other drivers involved in collisions with their policyholders.

Police also work closely with auto insurance carriers providing them with the official reports of specific accidents and with stolen car reports, which can be used to impeach a car owner who attempts to evade responsibility by claiming his car was stolen at the time it was involved in an accident.

The idea of provincial auto insurance has been put forward as a means for reducing the cost of insurance and some of the invasions of privacy occasioned by inspection of policy applications. In Manitoba, where provincial auto insurance has been established by law, three auto policies are mandatory: no-fault insurance, which is required for a driver's licence, and public liability ($50,000 basic) and collision ($250 deductible), which are required for motor vehicle registration. The no-fault insurance is weighted against young male drivers: $7 a year for a male over 25 and $3 a year for females over 25; $7 a year for females under 25, and $22 for males under 25. Accumulation of 6 demerit points for Highway Traffic Act violations incurs an annual surcharge of $50 while accumulation of the maximum quota of points costs $300 -- and this insurance is purchased on a 5-year basis. Public liability insurance premiums depend upon the age of the car, and owners of cars which become involved in accidents are liable for a surcharge. Moreover, in this province, the aged are subject to periodic re-examination to retain their driving privilege and the provincial mental hospitals and the blind institute make mandatory reports of admissions to the motor vehicle licencing authorities. It is interesting that Manitoba, which passed one of the first privacy of information statutes, then passed a provincial auto insurance act which stated that "prior legislation notwithstanding" the administrator of the provincial auto insurance plan can gather whatever information from government files he needs to discharge his duties.

It is apparent that insurance companies are adept principally at insuring themselves against loss. In so doing, they adopt a stance that can entail serious invasions of privacy. One wonders whether it has not become a case of information overkill, especially since we were told by an insurance company official that only seven per cent of all life insurance policies ever result in payment of a death claim.

CHAPTER 7

HEALTH SERVICES

INTRODUCTION

One of the most pervasive beliefs in the history of medicine is that the doctor-patient relationship is sacred, is essential for treatment, is a primary relationship, is confidential, and is free from third party interference. The doctor-patient relationship has been so structured that the patient will have faith in his doctor, and so be able to disclose the most intimate details of his life, and in turn allow the physician to give comprehensive medical treatment and care with compassion.

At least three trends are now in evidence which could fundamentally alter the nature of the traditional relationship: the new approaches in the delivery of care, the developing health information systems, and the changing status of the health professions. These trends have significant effects on the ability of the individual to protect the privacy of health information.

NEW PATTERNS IN HEALTH SERVICES

With advances in medical knowledge and techniques, a highly structured and specialized division of labour has emerged in the health profession. On the horizontal plane, the health professions are divided by training, responsibility, power and prestige into the

occupational categories of technicians, nurses, other allied health professionals and physicians. The number of categories increases with the size and complexity of the health unit with the limits ranging from the solo practitioner to a university medical centre. Over the vertical plane, the health professions are divided by clinical departments and specialties. The departments are limited in knowledge and practice to particular components of the health processes. It is not improbable that a single patient would give health and personal information, either verbally or through clinical tests, to all categories of health personnel. Moreover, if the patient has several problems, he may see a different set of professionals for each problem.

The central record in the hospital is the patient chart which is maintained at the nursing station. All notations and reports are entered on it, and all health professionals giving direct patient care have access to the chart. By reviewing the chart and by asking information from the nurse, intern, and/or resident, the physician in charge can make all medical decisions, possibly without ever seeing the patient.

In teaching hospitals, patients may be exposed to nursing and medical students as well. It is not uncommon for each member of a group of students attending clinical rounds to perform the examination procedure required. The results may be discussed by the group at the bedside without a single person speaking to the patient.

Not only are there more types of health professionals, but increasing specialization has resulted in more types of physicians. A person who has suffered a fall and goes to hospital may be seen by an orthopedic surgeon, a radiologist, an internist, a cardiologist, a neurologist, and a psychiatrist -- all on a consulting basis. Each specialist is interested in his "area" of the body so that the service rendered tends to be highly impersonal. Patient care in large hospitals has been criticized for being fragmented, to the point of being dehumanizing. The patient often is not told what is happening, why the procedures are performed, or what the results are. He is not even sure what information has been taken from him or who has it. This in turn leads to stress which can be deleterious to the therapeutic process (Duff and Hollingshead, 1968). Consequently some hospitals in the United States have appointed ombudsmen to represent the patients.

Group practices in the community may have lab technicians, R.NA.'s, R.N.'s, a public health nurse, physician, possibly a social worker, in addition to receptionists and secretaries. Again, the patients are processed through the health team chain so that the physician is last to see the patient. To a greater or lesser degree, the physicians gain information about the patient from the other health professionals, and the patient is not sure how much the physician knows when they begin talking.

In continuing visits, a number of persons sees the patient and accesses the file to update and retrieve information. For routine visits, decisions may be made and procedures performed without the physician seeing the patient.

In smaller practices, solo or partner, there is usually the physician and nurse-receptionist. This is probably the closest approximation to the ideal type of doctor-patient relationship.

There is an interesting emphasis to move the centre of treatment and education away from hospitals and into the community. Community practices and clinics are now beginning to train medical, nursing and social welfare students, in addition to interns and residents. The patients become the object of study and their records are the text. Both the Royal Commission on Health Services (1964) and the Ontario Committee on Healing Arts (1970) recommend that every individual be willing to serve as a "teaching patient".

Case examples are widely used in health education so that patients' medical records could be discussed at rounds, in lectures, and even at conventions. In some instances the patients are brought in to discuss their medical history and to answer questions. Videotaping and recording of doctor-patient interviews is being done widely, and the recordings are played back in a variety of settings. Finally, some teaching centres are building

one-way mirrors into examining room walls to allow the student to observe the clinical interview and procedures. As one might expect, not all of the teachers and physicians in training work to protect the privacy of the patients in these settings.

HEALTH RECORD SYSTEMS*

Health record systems have evolved in step with the advances in medical knowledge, procedures, and specialization. As treatment became more sophisticated and as more professionals became involved, records were necessary to ensure minimal co-ordination of patient care. In hospitals where attempts are made to evaluate the quality of care patients receive, the records of treatment rendered and tests performed are essential. The records can be used for other purposes, and these will be discussed.

---

* The writer relied, in part, upon James Stoddard, who is in the Federal Department of Communications and is working on the Computers and Communications Task Force, for information on the applications of computers in the health system of Canada. With increased number of applications in the health system, it is not improbable that significant applications were missed.

The quality of record systems in community practices varies more widely than the record systems in hospitals. If the studies by Clute (1963) and Peterson (1956) can be generalized, some physicians keep minimal records (a rare phenomena), some keep basic information, and some have developed systematic procedures for storing and using data. Group practices affiliated with universities are beginning to adopt more systematic records such as the E-Book and the Weed Records. The billing procedures required for provincial medical plans have probably done more to improve record systems in private practice than any other single event.

A Review Of Record Systems

There have been attempts in Canada to devise multi-use informational retrieval systems for health records. Listed below are some representative systems.

1. Psychiatric Case Register

   In the 1950's an attempt was made to establish a registry for all psychiatric admissions and separations in Canada which could be accessed by physicians throughout Canada. Apparently Ontario's refusal to participate prevented the system from being established. There are working psychiatric case registers in Maryland and Hawaii.

2. Southwestern Ontario Computer Council

It is proposed that 29 hospitals establish a computing centre with remote access terminals to process hospital records. The EDP activities in the order to be developed are: payroll, patient census, inventory, laboratory automation, accounts payable, general ledger, medical record indices, and advanced systems. Negotiations are presently underway to establish this system.

3. Hospital Activities Studies

(a) Professional Activities Studies and Patient Activity Studies -- PAS -- Ann Arbor, Michigan. Each subscribing hospital sends a completed form for each patient to Ann Arbor. Identification codes are used in place of doctor's and patient's names. Coded on the form are diagnoses and procedures used. The hospital in turn can add special categories and receive special tabulations from the program. Information is transmitted by mail. Approximately one-third of all Canadian hospitals subscribe to this service. The provincial government in Alberta requires that all hospitals in that province participate.

(b) Hospital Medical Records Institute-HMRI, was established by the Registered Record Librarians, the Ontario Hospital Association, and the Ontario Medical Association to provide the same service as PAS. About 15% of the hospitals subscribed.

(c) Other Hospital Systems

There is a group of hospitals in Hamilton beginning to use EDP systems for various record systems. It is not clear at this time how far or in what direction they will go.

In Regina, there is a regional centre which processes payrolls for eight hospitals. A grand design is lacking, but the computing facilities could be expanded.

The British Columbia Hospital Association has begun a sponsored computing service and 47 of the 147 member hospitals are involved.

The University of Toronto Teaching Hospital Association is considering developing an EDP system for its 12 members.

For some years, the Kings County Hospital in Brooklyn, New York, has operated the Obstetrical Statistical Cooperate (OSC). A number of hospitals, including some from Canada, send data to this system on all hospital terminations of pregnancies.

Toronto General, Hospital for Sick Children and Wellesley are developing in-house systems.

One of the more complete applications of computers in hospitals can be seen at El Camino Hospital, California (Feld, 1971). Patients are monitored by computers and notes can be entered into the patient files through a terminal at the viewing station. Physicians or nurses can review the patient's computer chart of any terminal in the hospital and update it with prescriptions or orders.

4. Registries for Cancer, Dialysis Patients, and Transplantations
Cancer institutes in British Columbia, Saskatchewan, Ontario, and Quebec are developing a general registry for Pap smears and on other reports of malignant tissues. Saskatchewan has two large cancer treatment centres which are undertaking longitudinal studies of survival, and the study includes linkages with other record systems.

Similar registries are being developed for dialysis equipment and patients with severe kidney disorders. There is an information exchange system so that if a suitable donor is available and permission is granted, organs for transplantation can be quickly transplanted to recipients.

5. Other Medical Systems

There is a group practice in Saskatchewan that is centralizing and computerizing its records. Each physician in the clinic will have access to a desk top terminal to retrieve information from a patient's file.

At MacMaster University, EDP is used for an epidemiological analysis of patients attending the family practice unit. In addition, G.D. Anderson, in the Department of Clinical Epidemiology and Biostatistics, has adapted the Conversational Computer Information and Statistical System (CCISS), originally developed at the University of Washington, so that it can be used in Health Science Centres in Ontario. He is distributing the software package at minimal costs so that research related health facilities can computerize their records.

Electrocardiograms (EKG) are transmitted by phone to Montreal and Toronto and interpreted by computer.

Laval University system provides 60,000 EKG interpretations a year. It is possible to use computer assisted diagnostic procedures by desk top terminal. Such a system has been developed by Dartmouth University but physicians seem to be slow to adapt its usage.

6. National Health and Welfare

The Department on National Health and Welfare currently maintains health information of the disabled, blind, rehabilitation clients, native peoples in some areas, people with communicable and chronic diseases, tuberculosis and venereal disease cases, migrants, public servants in hazardous occupations, commercial pilots, and various other individuals included in a departmental survey. The data are generally maintained on computer based files. They receive health information from provincial plans.

The department is planning a computerized health record. Development is on a system for the 35,000 people in the Northwest Territories. A commercial bureau would be located in Ottawa and could be linked to district health offices by terminals or telecommunication lines in the future. Information on the health of individuals, doctors, facilities and social problems (Alcoholism, drug addiction, etc.) would be processed by this sytem. It is probably the most extensive EDP health record system being planned to this date.

7. Provincial Medicare Plans

Most provinces are moving towards computerized record systems for health and hospital insurance plans. While most claims are currently mailed in and a batch processed, it is not beyond the realm of possibility that claims would eventually be entered by remote terminal or to transfer data on magnetic tape, particularly as hospitals are developing computerized systems.

Currently the provinces are using the EDP records for three purposes other than billing and accounting. The first concern is control over the type of medical care being delivered. Patients are asked to verify the charges against his account to make sure that doctors bill only for services performed. As the accounts are by the head of household's policy, the head of the household may receive billings for his wife and children as well. This technically prevents the wife and children, particularly teenagers, from establishing a confidential relationship with the doctor.

The records are used to monitor the volume of practice in addition to type of service rendered, so that the governments can begin to undertake cost benefit analysis of the health system. Records for hospitalizations may be used in a similar fashion.

The second basic purpose is research into the epidemiology of diseases and patterns of health care utilization. While such research can be based on aggregate data which are not individually identifiable, use of identifiable files is preferred. In one province a researcher was able to interface medicare data with a magnetic tape of income tax returns to study the socio-economic correlates of disease distribution and health services utilization.

The use of the data for these purposes is necessary to evaluate the impact of new health services on an area and to help plan new services. Again, the belief is that the public gains more than it loses.

The third basic purpose of such data is to help enforce legislation. In Manitoba the medicare records are interfaced with driver's license applications to ascertain if the applicant should be refused a license for health reasons. It is technically feasible to interface health records with records of other government agencies to assure that legal requirements and restrictions are met. This would be particularly true as health reasons are often used in applications for welfare and other forms of social assistance.

8. Provincial Public Health Departments

Every province requires physicians to report cases of infectious, communicable, and other diseases or conditions which threaten the health and well-being of the public and the individual involved (such as epilepsy, alcoholism, suicide attempts, and traumatic injuries caused by violent acts). There may be clinical epidemiological follow-ups for purposes of primary, secondary, and tertiary prevention of additional health problems.

Venereal disease and tuberculosis are two specific areas where clinical field investigations involve not only the patient, but his immediate family and his contracts. The individuals are legally required to seek treatment.

Public health departments may frequently work with school systems to provide basic health services for children. The clinical findings can result in follow-up visits in the home and involvement of the family.

As with the other provincial uses of health information, the perceived benefits to society outweigh the disadvantages individuals may encounter when they are clinically investigated.

9. Insurance Exams

Before most individuals can be insured, they are required to take physical examinations, usually by a doctor specified by the insurance company. The health information not only helps to determine whether insurance will be granted but also may be used to determine the rates the approved applicant must pay.

If an applicant is refused for health reasons, his name is submitted to the Medical Information Bureau, an exchange service located in Boston which is operated by insurance companies in North America. Reports are routinely published and circulated to other companies. Insurance companies routinely query MIB to make sure applicants have not been turned down by other companies.

Retail Credit of Canada participates in the inspection of life insurance applicants so that refusal of life insurance for health reasons may become part of a dossier on an individual. Such dossiers are frequently used in personnel and credit clearance procedures.

The possible applications of computer assisted health record systems can be summarized as follows (McLachlin and Shegog, 1968; Rose, 1969):

1. Basic Accounting procedures -- Billings for services rendered.

2. Classification of Records -- Categorizing health records by problem areas.

3. Diagnosis and Clinical Interpretation -- It is possible for electrocardiograms and electroencephlograms to be transmitted by satellite and analyzed by computing centres in remote cities. Computers can be programmed for the necessary pattern analysis.

4. Case History -- By using a two-way conversational terminal and a programmed series of questions, the computer can take a complete medical history.

5. Treatment -- The physicians can feed in a series of symptoms, and through a clustering procedure the computer can analyze the problems and prescribe treatment.

6. Case Registry -- Cancer institutes use registers to allow for follow-up of cancer patients.

7. Record Linkage -- The linkage of records from all health facilities allows for the study of the flow of patients through the health care systems. Provincial medicare insurance plans allow for such linkage, and the Ontario Council of Health has proposed the usage of records for this purpose.

8. Control -- The vital responses of a patient in an operating or intensive care room could be monitored by a computer and automatic adjustments could be made. Secondly, by studying diagnosis, cost, length of stay, treatments received, and attending health professionals; financial and professional controls could be exercised. Finally, health records can be linked with records in other sectors for certain type of financial and government control.

9. Research -- Centralized records and EDP have provided an abundance of materials for epidemiological, cost-benefit analysis, and other public health related studies. Evaluative research of health programs can become an integral part of program operations.

It is apparent that in Canada, health record systems are being planned or implemented that in one manner or another, include all nine of the above possibilities.

Questionnaire Data from Health and Vital Statistics Organizations

One hundred and eighty-two health and vital statistics organizations completed the questionnaire sent out by the Task Force. In order to preserve the privacy of the organizations, they were not identified so that a more detailed breakdown is not available.

Most of the reporting organizations had around 500 employees (39% had 100 to 500 employees and 23% had 501 to 1,000 employees), less than 25,000 clients (33% had less than 2,000 and 30% had between 2,000 and 25,000) and between 25,000 and 100,000 records (60%). Only 42% used computers.

Only 59 of 182 organizations allowed the subjects to see their own files; 34 allowed them to see the complete file. Over 80% reported less than 500 outside requests for information a year.

In obtaining information for the files the key sources, aside from the subject, were medical practitioners, hospitals, and family, to a lesser degree. Police and investigators were infrequently used. Most organizations (over 85%) attempted to control misuse of records, but less than 20% were effective in terms of catching and disciplining staff.

The records of the health and vital statistics organizations were stored mainly in the province (83%), to a lesser degree in Canada outside the province (less than 10%) and only about 5% partially stored records in the U.S. Between 35% and 40% of the organizations exchanged information with agencies in the United States and only 10 did so frequently.

It should be remembered that the records included employees as well as clients, and that we do not know what items of files may be transferred to other individuals or agencies. Most health and vital statistics organizations maintain extensive, hard copy files. The size and bulk of the files make rapid and multiple access unlikely; while some records may be definitely misused, this probably is not done either extensively or systematically. As health and vital statistics organizations computerize their records, there will probably be major reformations of policies concerning record keeping systems.

Particular Problems with Psychiatric Hospital Data

A particular health agency needs data for service, teaching, research, planning, and control; and this is true for a private practitioner as well as a large hospital. However, before data are gathered there is an assumption that there is a need for the data and that the cost of collection is acceptable. While the issues of need and cost are omnipresent, the problems are decidedly greater for psychiatric hospitals. The brief from Clarke Institute of Psychiatry, in particular, delineated the issues involved.

Psychiatry is an uncertain art. The causes and cures for most forms of mental illness are unknown. There is an implicit assumption that if more data on patients could be collected and processed, they would assist in clinical management and etiological and epidemiological, mental health research.

The direct cost of collecting psychiatric data is rapidly being reduced. Researchers are developing standardized forms for the collection of information. Computer systems have enabled psychiatric hospitals to have running records of patients. There is a potential cost to the patients in terms of confidentiality. The researchers are aware of the security systems available for EDP data banks, and they acknowledge that confidentiality cannot be absolutely guaranteed because of the number of staff members and the vulnerability of EDP systems.

The need for data is best demonstrated by reliability and validity; that is, the data can be used for understanding, prediction, and control. However, psychiatry has not even been able to describe and evaluate emotional problems; the diagnostic nomenclature has not been standardized. Furthermore, with the dynamic and holistic approach to personality, information on all facets of the patient's life is explored. The data, to this point, have not been related to psychiatric disorders with a high degree of reliability and validity.

Hospital data are of limited use in etiological and epidemiological research as only a small proportion of individuals has mental problems and as there is little continuity with the information gathered by practising physicians. The data, at this point, are of more value in the areas of planning and control than in the areas of teaching, service, and research.

The social and legal consequences of psychiatric treatment are greater than for any other form of health services. Because of the breadth and depth of the potential personal information which could be gathered, the costs are high, both in terms of finances and possible breaches of confidence. At the same time the need for the data has been questioned.

In their brief to the Task Force, Drs. H.B. Kenward, M.R. Eastwood, and F.W. Furlong concluded, "... that a central computer bank is potentially beneficial to psychiatric practice and research but believe that such a scheme cannot be incorporated until prior studies on validity and reliability have been carried out."

IMPLICATIONS OF COMPUTERIZED SYSTEM

Introduction of a broadened base for health care, both in terms of personnel and technology, has numerous implications for our society. Ray N. Freed (1970) has examined the legal implications of computer assisted diagnosis, computer performance of medical procedure, computerized patient simulation, and computerized hospital records in terms of the practitioner, the system's operator, and the system manufacturer. Most of the discussion focuses on liability arising from malpractice and the delegation of medical responsibility. There is no legislation in Canada to assure the privacy of health data. The problems of

transmission of incorrect information and authorized release of information are considered from the perspective of the privacy of the patient. Freed's discussion centres on failure within a particular system with no consideration given to problems that would arise when health systems are linked and records from several systems, medical and non-medical, are interfaced.

There are three basic dimensions to the problems arising from information exchanges in the modern health systems: the probability of error, the loss of control of personal information, and the third party use of health information resulting in implications which are often deleterious to parties involved.

Accuracy of Records

Where computers have been applied, minimal consideration has been given as to the information to be included and its predictive information. If information is included it should be needed. Consequently, it must be accurate and current (Kenward, et al., 1971). Even if the information which has been gathered is accurate, two basic sources of error in medical records remain, the diagnoses and reporting of findings. First, it must be recognized that diagnoses are probability statements. Initial health complaints may be indicative of a wide range of health problems. By eliminating certain possibilities and gathering additional information, by medical history or clinical tests, the

physician limits the range of possible alternatives. As diagnosis is generally viewed as a necessary step preceding treatment, the decision to affix a diagnosis to a particular set of symptoms implicitly involves the assessments of risk (Lusted, 1968; Fox, 1959).

From the general practitioner's office most complaints are non-specific in origin and there is low probability of immediate danger to the patient. Diagnoses are used for billing purposes and treatment is given to meet the expectations of the patient. The general assumption is that it is better to diagnose and treat the patient unnecessarily than to risk missing a serious condition. As most patients do not return for a second visit for the same complaint, the physician seldom has a chance to follow up. The whole program is compounded in that half of the complaints seen by a primary physician are psychosomatic in origin.

As individuals undergo clinical and laboratory tests, the probability of an inaccurate diagnosis increases, but the costs of the test increase more rapidly than probability errors decrease. Even with serious conditions such as heart disease, cancer, and respiratory conditions, the diagnoses may be right more than 90% of the time. The key point, however, is that a significant proportion of diagnoses are inaccurate.

Physicians may use deceit in completing medical records. If a patient has venereal disease or if the physician suspects alcoholism or childbeating, he usually does not report such conditions because of legal implications for the patient. More socially acceptable findings are recorded on the reports. The main point is, one cannot assume that record health information is reliable or valid.

Control of Information

Once the health information record enters a multi-access data bank, the individual loses control of the information. Innumerable individuals have access to and use the information without the knowledge of the subjects on record. Computerized records increase the numbers of users of information, and the printout can form the core of new data banks. Files are reproduced by electrophotic equipment, and there is usually no attempt to account for the materials once circulated.

The information a physician receives is ethically privileged and is the end product of a confidential relationship. Intimate details are transmitted only when the person is convinced the information will not be circulated or misused and that he will continue to be respected. If the information is then converted to a form suitable for other purposes and becomes a part of a health information retrieval system, then the patient loses control of information and potential uses of that data.

Curran, and his associates (1969) in a review of Massachusetts legislation pertaining to health information, found that degrees of confidentiality are recognized. These findings can be summarized as follows:

Degrees of Health-Record Confidentiality

Not Subject to Subpoena:

Clinical psychiatric records.
Research studies designated by the Commissioner of Public Health as confidential.
Records concerning applicants for vocational rehabilitation.

Highly Restricted:

Venereal disease records.
Vital statistics records.
Industrial accidents.
Public Welfare Department records.

Generally Confidential:

Hospital and clinic records.
Clinical patient records of physicians.

Non-confidential or Public Records:

Vital statistics.
Dangerous disease reports.
Acute-poisoning reports.
Battered-child reports.
Vehicular accident reports.

The degrees of confidentiality are not generally enforced. There are variations from one state and province to another, so that what may have a high degree of confidentiality in one area could

have a lower degree in another region. Nor is there any legislation which limits circulation of health information through businesses and private agencies. While there are many states which have legislation guaranteeing the confidentiality of the doctor-patient relationship, no such legislation exists in Canada.

Social and Legal Consequences of Health Problems

It is recognized that health problems can result in limitations of activities. The social consequences of the condition may exceed actual limitations. Some diseases carry stigma, and a person with those conditions is discriminated against. Persons who are blind, deaf, deformed, mentally ill, cancerous, or non-medical users of drugs can attest to the negative social consequences of the conditions.

In employment procedures, it is clear that health information is becoming as important as age, education, work experience, and social heritage. Large businesses have medical departments and/or security offices which look for health problems that might affect work or serve as indicators of unfit character (psychiatric problems, venereal disease, drinking problems, non-medical use of drugs). Negative health information may result in the loss of job possibilities and life chances.

The breath analysis law which is designed to stop drunken driving has raised controversy in which it is alleged that a person has to give testimony against himself. Yet there are a number of health areas with similar legal requirements; psychiatry, venereal disease, and tuberculosis are but a few examples. The health professionals use their patient-professional realtionship to gain information and then give the information to use against the individual (Szasz, 1965).

The designs of developing health record systems mean the information obtained from the doctor-patient relationship extends the possibilities of usage of the data. The health professionals are becoming more the agents of society and less the confidents of the patients.

In summary, if there is questionable medical evidence, it can no longer be assumed that it is better to diagnose and treat than not to make a medical decision. Before data are entered into the health record system, both the patient and the physician should clearly understand who will use the medical records and for what specific purposes. The consequences of the resultant diagnoses should be understood. Individuals having insurance examinations should recognize that the information may well be used for credit and personnel purposes. Physicians in given provinces must realize that diagnoses used on billing forms are to be reviewed when patients apply for driver's licenses.

At least some health authorities believe that privacy and confidentiality of health information will become a dead issue with the public.* However, another possibility is that the individuals will become increasingly reluctant to give health information. The public response to the loss of confidentiality and privacy is essentially unknown.

DATA BANKS AND HEALTH PROFESSIONALS

There has been a general view held that lower status members of society have less privacy than higher status members. In the university study and the site interviews, it has become apparent that the converse is true. The account of information maintained on individuals is directly related to the educational requirements, power, and prestige of the individual's occupational category.

By and large, the health professions have the responsibility for setting the criteria for admission to professional schools, for accrediting the schools, for approving clinical training facilities, and for the examination procedures required for licensing. Consequently, the professions have set up elaborate record systems to assure the criteria are met.

---

* Provincial public officials recently expressed this view in a conference on venereal disease control. In some circles, this view is becoming very widely accepted.

Generally, the health professional schools require more extensive background data on applicants that non-professional educational programs. Letters of recommendation which contain references to personality characteristics, attitudes, motivation, and industry are given heavier weight for applicants to medical, dental, and nursing faculties than in the arts and science faculties. Personal interviews may be required for potential health students and not for others, and the interviewers' summary comments can be of critical importance. Professional health faculties are much more likely to require standardized test scores of applicants than of other programs.

The same pattern follows throughout the professional careers of physicians, dentists, and nurses. As physicians are at the pinnacle of the health professions, the records maintained can serve as a guide for the others.

Applicants to medical schools may have to submit applications calling for academic data plus work history; financial position and Medical College Aptitude Test scores (MCAT) are generally required. The letters of reference are obtained, and if the students pass the initial screening, they will be summoned for a personal interview during which the interviewer may explore any dimension of personality or professional interests. The interviewer's notes are placed in the dossier.

The Association of Canadian Medical Colleges (ACMC) has a continuing research program whereby extensive data are collected on every applicant to medical schools in Canada. The socio-economic data sheets are included with every set of application forms. The sheets are to be returned to the office in Ottawa directly, but some admission officers have abstracted information from them information which could not be on the application as it contravenes the spirit of the human right codes. ACMC collects MCAT scores and pre-medical academic records as well. Several research reports have been published based on the analysis of the data.

Consideration has been given to having medical students take psychological tests so that the scores can be added to the files. The University of Toronto now has its medical students complete such a test. Medical academic records could be added and the ACMC files could become historical records.

Student evaluations and academic progress are assessed by faculty committees and any action taken on every student, from continuance to supplemental exams to termination, is reported to the Faculty Council. Student standing and class rank are disseminated widely in the college.

Numerous entries are made into the historical hard file, which is maintained in the dean's office. Student files are open to faculty members.

As the student approaches Medical Council of Canada examinations, new files in new offices are created. Before a medical student can be licensed, he has to pass the Medical Council exams. After his fourth year, MCC keeps records to determine the student's eligibility to write the exams and the performance on the exams.

In addition to graduating from an accredited medical school and passing the exams, the student must serve an internship of one year in an accredited hospital. As the competition for internships at prestige hospitals is keen, the hospitals collect extensive information from the medical school and letters of recommendation from faculty. The candidate may again be interviewed with assessments entering the file.

After the internship, the physician seeks his license to practice from the provincial College of Physicians and Surgeons. They in turn gather extensive information to assure that the candidate is eligible.

All physicians become members of the provincial Colleges of Physicians and Surgeons, and most join the provincial medical association which, in turn, create files. The Colleges of Physicians and Surgeons serve as disciplinary bodies responsible for sanctioning their members for unethical practices.

If physicians pursue specialization certification, there is another round of applications for residencies in hospitals and certification exams with the creation of additional files. When the physician goes into practice, he usually seeks to join the medical staff of a hospital, and another professional dossier is formed.

Under the provincial medicare scheme, most physicians join the plan. To do this another professional file is created. The provinces have developed cost-control uses for these files. The billing and treatment procedures are analyzed by a physician. If there are significant disparities, the provincial authorities may refer the list of questionable physicians to the colleges for review for disciplinary action. In some instances, the provincial governments have threatened to take direct disciplinary action if the colleges are reluctant to act.

In the Province of British Columbia the government has considered assuming control of granting of hospital staff privileges. Such provincial control would break the professional monopoly and would serve as a means to redistribute the physicians in the province.

The Ontario Committee on the Healing Arts has recommended that more be done to hold physicians publicly accountable for questionable medical practices and unethical acts. Their recommendations include increased public participation in discipline proceedings.

As mentioned earlier, the Department of National Health and Welfare has formed a Health Manpower Resource group which is to study the professional patterns and geographical distributions of health professionals in Canada. The nature and extent of their files are unknown.

This basic overview of records on physicians could be extended to other health professionals. The main differences would be that generally the professional training period is not as long or as complex for dentists, nurses, technicians and other health professionals as for physicians. Of all the health professionals, physicians are probably the most powerful and prestigious. Probably more information is maintained on physicians than on any other category of health professionals.

HEALTH INFORMATION: INTELLIGENCE AND CONTROL

After the government decided that health was a right to be guaranteed, health became a concern which has grown in importance. Health costs continue to increase at a rate faster than other economic sectors of society. The entire health industry, suppliers, facilities, and professionals, has come under severe scrutiny.

As provincial governments have assumed direct control over medicare insurance plans, they have attempted to control costs while improving service. Governments are attempting to rationalize service by pitting benefits gained against the costs of various programs and practices. The system has evolved to where the health professions shape and control the operations while the government has the responsibilities of finances and responding to public demands. It almost appears that from the perspective of government, the doctor-patient relationship is disfunctional in that it perpetuates physician control.

If one can assume that financial responsibility tends to lead to control, then it follows that health professionals would tend to become adversaries of the government. As a part of the contest for control, both the professional bodies and governments are developing information retrieval systems that will allow for feedback and control. There is an assumption that intelligence is a necessary part of the deliberation. As a consequence, more information is probably maintained on health professionals than any other occupational category in society.

As previously suggested, the intelligence issue does not stop with information on physicians, but it includes the use of patient data as well. There are the basic questions of how much information is needed and who needs to know. The question of intelligence for control has become more important than the question of the right of the individuals on whom the data is stored.

Intelligence, health, and privacy are not necessarily related, one or two of the concepts could be promoted at the expense of the remaining concept(s). It is not clear to what extent they are interdependent or mutually exclusive.

SUMMARY

Since 1960 there have been significant changes in the health field. The federal and provincial governments have moved to guarantee the right to health regardless of age, race, social status, or place of residence. Closely related is the push to move medicine out of the medical centres and into the community and home, and as a result allied health professionals are being called upon to assist. Second and third generation computing equipment allow for medical data banks with rapid and multiple accessing of records, allowing community centres services that were before only available to the medical centres. The government financial interest in the health field is leading to greater control.

As a result of the process the confidentiality of medical records is constantly being questioned if not observed. It appears that the changes are taking place without privacy being considered except as an afterthought. At this point in time the issue of confidentiality and privacy is an open question, the answer will come as the medical record system develops.

References

Canadian Medical Association, Letter from B. E. Freamo, Executive Secretary, to the Task Force, June 30, 1971.

Clute, Kenneth L. The General Practitioner: Study of Medical Education and Practice in Ontario and Nova Scotia. Toronto: University of Toronto Press, 1963.

Curran, Williams J. et al. Privacy, confidentiality and other legal considerations in the establishment of a centralized health-data system, New England Journal of Medicine (July 31, 1969) 281:241-248.

Feld, Roger. Computers enter medicine, New York Times.

Fox, Renee C. Experiment Perilous: Physicians and Patients Facing the Unknown. Glencoe, Illinois: The Free Press, 1959.

Freed, Roy N. Legal aspects of computer use in medicine, Law and Contemporary Problems (1970) 35:674-706.

Hilmar, N.A. Anonymity, confidentiality, and invasion of privacy: Responsibility of the researcher, American Journal of Public Health (1968) 58:324-330.

Kenward, H. B., Eastwood, M. R., and Furlong, F. W. Computers and psychiatric data recording: A discussion of the problem of confidentiality and other associated issues, Brief from the Psychiatric Epidemiology Section of the Clarke Institute of Psychiatry, 1971.

Lusted, Lee B. Introduction to Medical Decision Making. Springfield, Illinois: Charles C. Thomas, 1968.

McLachlin, G., and Shegog, R.A. (Eds.) Computers in the Service of Medicine: Essays on Current Research and Applications. Volumes I and II, London: Oxford University Press, 1968.

Ontario Committee on the Healing Arts, Final Report. Three Volumes, Toronto: Queens Printer, 1970.

Ontario Council of Health. Committee on Health Statistics, Part I: Health Statistics System, 1969, Part II: Implementation, 1970. Toronto: Queens Printer.

Ontario Medical Association. A report of the committee on the application of computers to medical practice. A Brief submitted to the Task Force, July 21, 1971.

Peterson, Osler L. et al. An Analytical Study of North Carolina General Practice, 1953-54. Evanston, Illinois: Association of American Medical Colleges, 1956.

Rose, J. (Ed.) Computers in Medicine. London: J.A. Churchill Ltd., 1969.

Royal Commission on Health Services. Final Report. Two Volumes, Ottawa: Queens Printer, 1964.

Schwartz, William B. Medicine and the computers: The promise and problems of change, New England Journal of Medicine. (December 3, 1970) 283:1257-1264.

Smedeker, Lendon. On confidentiality and data banks, New England Journal of Medicine (July 31, 1969) 281:269-270.

Szasz, Thomas. Psychiatric Justice. New York: The Macmillan Co., 1965.

Weed, Lawrence L. Medical Records, Medical Education and Patient Care. Cleveland: Case Western Reserve University Press, 1969.

Site Interviews

Clarke Institute of Psychiatry

Dominion Bureau of Statistics

Federal Department of National Health and Welfare

Notre Dame Hospital

Ontario Health Services Insurance Plan

Plus other site interviews in which health data were discussed.

CHAPTER 8

EDUCATION

The handling of individually identifiable records containing personal information takes on important long-range social significance when these records concern or describe students, because it is an important part of the learning process that these young and impressionable people be justly treated by an establishment that asks their respect and even more important that they perceive themselves to be justly treated.

This section draws upon a study of the handling of student records in Ontario universities by Carroll and Williams in 1970. The study was supported by the Canada Council, Social Science and Humanities Division. The investigation entailed making site visits to 14 provincially supported universities in the Province of Ontario. In addition, 19 Canadian universities outside of Ontario responded to a detailed mail questionnaire distributed by the investigators.

The fact that undergraduate university students are concerned about real or imagined invasions of privacy by computerized records was made abundantly clear in at least two student-establishment confrontations in Canadian universities (1968 - 70).

The handling of student records was likewise one cause of persistent intra-administration vituperation in two universities in Ontario during the same period.

The burning of the $1.6 million CDC-3300 computer at Sir George Williams University by dissident students on January 29, 1969 and the concomitant destruction of university records, registration cards, and transcripts has been viewed as a neo-Luddite reaction as well as a strategy to wreck the university by destroying its critical function, its computer centre.

The handling of student records was one subject of student-administration dialogue subsequent to an undergraduate sit-in at the University of Windsor. A result of this dialogue was publication of agreed-upon guidelines for the acquisition, handling, and dissemination of personalized information concerning or describing students. It is noteworthy that, at the time of the 1970 Carroll-Williams study, the University of Windsor was one of only two provincially supported universities in the Province of Ontario having such an articulated policy regarding student records.

During the same period, at Lakehead University, intra-administration dissonance relating to the handling of student records and transcripts resulted in this function being withdrawn from the cognizance of the university Registrar's Office and placed under control of a new office created for this purpose.

Furthermore, at Laurentian University there was a confrontation between the university Senate, faculty, and student body, on one hand, and the former President and Board of Governors, on the other. The handling of student records figured in a minor way in this dispute.

Analysis of responses by organizations to the Task Force questionnaire indicated that educational institutions supplied about 16% of personalized information exchanged among organizations while receiving only about 5% of this information from other organizations. Twenty-one per cent of respondents said that they received personalized information concerning or describing individuals from educational institutions the individuals had attended. Among the 26 categories of organizations classified as to function, educational institutions ranked as second most likely to release personalized information concerning or describing individuals. Educational institutions were ranked as third most likely to receive complaints from individuals or groups representing their interests regarding the disclosure of such information.

Educational institutions were ranked sixth among functional categories of organizations most likely to receive complaints regarding the collection of personalized information. They were ranked seventh most likely to receive complaints arising from the inability of individuals to examine the contents of records containing personalized information concerning or describing them.

However, privacy of student records means different things in different contexts; the concept of privacy is heavily influenced by the traditions of particular institutions. What may be a gross invasion of privacy at one university is accepted as standard practice at another.

The most stringent measures are taken at some institutions to ensure that course marks remain a confidential matter exclusively between the student and faculty member directly concerned. In other institutions, marks lists may be circulated to all faculty, posted on bulletin boards, published in newspapers, and, in one case, declaimed publicly by the dean from the front steps.

There have been outcries by student groups against the university collecting data on students regarding race, religion, national, or socio-economic origins for fear of these facts being used to discriminate unlawfully against some students. Yet, at other times, perhaps the very individuals or groups who launched the initial protests will request an assessment of the number of native people enrolled for higher education, the number of non-Roman Catholics admitted to some erstwhile Roman Catholic university now under provincial control, the number of students of working-class origin at university, or the number of Americans in Canadian graduate schools.

Some schools tend to regard themselves as an educational supermarket where students come, pay their fees, and leave with their course credits. Others see themselves as truly an alma mater, actually standing in loco parentis, and consequently assume a paternalistic stance. In such schools, the masters of colleges become intimate advisors to their students and are furnished with detailed dossiers about them to aid in counselling activities.

Central to the problem of privacy of student records is the lack of enunciated policy regarding privacy. In our study of 14 provincially supported universities in Ontario (1970), only two furnished us with copies of statements of university policy regarding privacy. Only one of these furnished copies of student consent forms to initiate such release of information.

Documentation released outside of a university consists in part of transcripts of academic records and letters of recommendation from faculty. Transcripts are usually certified Xerox copies of a permanent transcript card to which are affixed computer-produced sticky labels giving course numbers, credit values, and marks. (This system affords opportunity for forgery). Many transcripts include a recapitulation of secondary school marks. A transcript is released upon request of a student and sent directly from the registrar to the employer or institution seeking it.

Letters of recommendation in support of a student's application for some benefit such as a job or admission to another institution are solicited from faculty by the student and sent directly to the firm or institution concerned. Seldom can faculty bring themselves to write unfavourable letters. At worse, they damn with faint praise and in a pseudo-code only the cogniscenti can decipher, to wit:

"Works well when properly motivated"	(lazy)
"Excells in oral communications"	(can't spell)
"Performs well in qualitative studies"	(can't add)
"Pleasant fellow, plays tennis well"	(just plain dumb)
"Displays a lively interest in his environment"	(leads protest marches)

In one province, which recently abolished provincially set secondary school leaving examinations, universities have been establishing the practice of sending periodic reports on the progress of former students to their former secondary school principals, who are apparently looking for new predictors of success among prospective university students. Some students, who were not especially happy in secondary school, have expressed displeasure with this practice.

In response to other inquiries regarding matriculating students, registrars will usually only confirm the fact of enrolment. However, student councils often publish and sell student directories -- at three universities these included names, addresses, telephone numbers, marital status, and photographs, until the prettier coeds began receiving obscene phone calls (1968).

Much information is obtained from the campus by informal contacts. Campus police establish working relationships with local police. Such contacts have also been established with faculty members. Much of this information gets out by telephone. One professor reports receiving calls from an automobile insurance carrier and from the telephone company credit office to confirm that particular students were carrying "B" averages. This fact appeared to be of some consequence in establishing the premium for automobile liability insurance and in establishing the students' eligibility to receive telephone service.

Research activities of social scientists frequently invade the privacy of students. One study concerned room-mate compatibility and students had to answer a detailed personal questionnaire before being able to obtain residence accommodation.

In many universities, ethics committees have been established to screen plans for such studies.

On the university level, a serious problem in processing student records lies in casual handling of computer-produced hard copy records and lists.

Thus, despite the establishment of central records offices no such group can be said to have real control over student records.

The computer is frequently used as a million-dollar typewriter: in records processing, its computational use is minimal. Instead, it produces a succession of preliminary copies, confirmation copies, verification copies, etc. -- in duplicate, triplicate, and more. This production of multiple, unaccounted hard copies is abetted by promiscuous use of the Xerox machine.

The result is that in addition to the central records facility, every dean, department chairman, administrative aide, and faculty member builds up a private file (of varying size) of usually incorrect or outdated information, at a waste of his own or his secretary's time, and kept under conditions of dubious security.

Several violations of confidentiality were reported to us:

. A janitor used spoiled print-outs of course lists with preliminary grades to line office wastebaskets.

. A secondary-school student learned his secondary school final marks before his school released them, through a source in the Registrar's office at a university to which he had applied for admission.

. Lists of new admissions were given to an office (Student Health) other than that of the Registrar before the Registrar received them. As a consequence, applicants were sent implied notice of admission in mailed circulars before official notifications were released.

. A Student was able to tell his dean his class standing before standings were officially announced; the student had obtained an advanced print-out of the course list sent to one of his instructors.

The greatest problem in storage of student records lies in collecting too much information and storing it too long. This not only contributes to possible invasion of student privacy but also is uneconomical.

Despite substantial progress to the contrary, we found universities that persist in collecting information which may be utilized to establish a students' religious persuasion, ethnic origin, or socio-economic status. These questions include:

- religion
- country of birth
- language spoken (as opposed to proficiency in the language of instruction)
- father's (mother's, relative's) country of birth
- date of entry into Canada
- previous names
- father's occupation
- are parents alumni of this university?
- are parents (relatives) college graduates?
- father's employer
- city, country, and province of birth
- number of siblings older and younger
- marital history of student (divorces, etc.)

In general, university medical officers, awards officers, and counsellors maintain separate files only a few of which have yet been computerized. Some suggestions have been made regarding the eventual establishment of master student data banks but these suggestions have yet to be adopted.

A large proportion of most student master records is filled with information originally collected to arrive at an admissions decision.

These admissions data include:

- principal's rating
- secondary school marks, grade 12 and below
- standard test scores
- prior academic history
- grade 13 marks (in Ontario)
- previous applications to university
- work history prior to admission
- comments made at time of admission

There are vast individual differences among university admissions officers with respect to how much data is acquired before an admissions decision is made.

- All Ontario universities utilize a standard provincial admission form which is forwarded directly to the university admissions officer from the secondary school guidance officer.

- Many universities supplement the standard application form with their own locally designed form. This form is used in place of the standard Ontario form in the cases of mature applicants. It requires a detailed personal work history, presumably to assure the admissions officer that the mature applicant has not spent the time since leaving secondary school unsuccessfully matriculating in some other university.

. Some universities acquire additional personal data from the applicant on a special information form, which may be used in place of, or in conjunction with, the university's supplemental application form.

. Nearly all universities require mature applicants to write a special examination.

. Several universities require the applicant to furnish names and addresses of references who are then requested to provide confidential appraisals of the applicant. This is more common in the case of mature applicants than applicants coming directly from secondary school.

. Some universities require the applicant to undergo a medical examination prior to admission. Often this is required only of prospective physical education specialists.

The sharing of computer facilities between the custodians of confidential information and students learning how to programme computers creates several unique opportunities for breaches of security.

Our studies showed that, in the majority of cases, the same computer used to process administrative data was also used for academic instruction and research.

	Ontario	Outside Ontario
Same Computer	9	12
Separate Computer	4	5
No Computer	1	2
	14	19

In general, the computer used for teaching and research is highly visible and consequently vulnerable, as was demonstrated in 1969 at Sir George Williams University. The computer room usually has at least one glass wall. There are frequent tours by undergraduate Computer Science classes. Students, graduate students, and junior faculty and staff frequently work as programmers or operators. Senior Computer Science students may be allowed to programme the school's computer in machine language, frequently causing monitor crashes.

Back-up tapes of student records are often stored within the computing facility. Historical records, however, are kept in storage cabinets and document boxes. Little use is made of microfilm for storing these records.

Canadian universities are entering a new era of data processing and Ontario is apparently leading the way. They are moving from centralized batch processing of records to concepts of data processing which involve functioning in resource-sharing remotely-accessible computer environments.

Our survey (1970) revealed the following means for processing student records:

	Ontario	Outside Ontario
Some form of remote access	6	1
Remote capability or plans to employ remote access	6	5
Batch processing exclusively	2	10
No computer processing	0	3
TOTALS	14	19

Among the 7 universities with some form of remote access to student records we observed several variants in processing:

Mode of Processing	Number of Universities
Remote high-speed data entry	1
Remote keyboarded data entry	1
Remote display of selected records	3
Remote high-speed entry, printer output, and display	1
Remote display and keyboard update	1
TOTALS	7

The 8 Ontario universities not presently using remote access require some additional breakdown:

State of Development	Universities
Plans to go remote, no existing capability	3
No plans to go remote, existing capability	2
No plans to go remote, no existing capability	2
Plans to go remote, existing capability some developmental work	1
TOTALS	8

Remote access to student records presents both advantages and hazards from a security point-of-view. On the positive side, it does away with the multiple printouts that probably constitute the greatest existing threat to confidentiality. On the other hand, the remote computer has no way of telling whether the user at a terminal has a right to the information he has requested to see, and more seriously, to alter or update. Nor can the computer tell, in some cases, whether the request came from a legitimate system terminal. It should be noted also that the user at his remote terminal has no positive means of assuring himself that he is really in communication with the right computer. There is the additional hazard of potential wiretapping on telecommunications lines.

In one provincial university system which was visited by the Task Force (Université du Québec), the student population is 10,000 distributed among three universities. Records exist in both manual and electronic media. During the admission request period the manual record contains an admission request form which includes name, address, and sociological information; birth certificate (not required at all universities), picture of student (not required at all universities), previous school records, results of admission examination (required only for mature students at many universities), and the results of an initial interview (not required at all universities). Not noted here but required by some universities is a recommendation from the secondary school principal.

If the student is admitted and registered, the record is augmented with an admission answer or acceptance to a specified programme, registration, and subsequently academic data including test results, progression from year to year, evaluations, and sanctions (at some universities the last two types of information are not made part of the student's permanent record).

Student records in manual form contain no accounting information; it is kept in the accounting department. Admission requests without subsequent registration are kept two years then microfilmed and transferred to the archives as are records of students who withdraw or graduate. Students may consult their records and have them corrected if found to be in error.

There are two computer files. One contains records of all students applying for admission; it facilitates detecting students who apply simultaneously to two or more constituent universities. The other contains records on all registered students and includes accounting information. Plans have been made to place the files on disks with direct access from all constituent universities. Controls implemented by keys and passwords will limit each university's access to the system to its own student records. Appropriate hard-copy listings go to the registrar and accounting office of each constituent university.

Record keeping for secondary and primary schools is tending to become computerized on a district basis. But computerization of existing school records is like outfitting a flabby frump in a couturier creation. Records are based upon a jerry-built format incorporating every item of personal information that generations of counsellors have thought might help them better understand the child. Thus there is space for photographs; family background information of a socio-economic, cultural, and ethnic character; psychological test results, career goals, and outside interests; teachers' comments, as well as marks. These manual records are generally supposed to be confidential but we have been told of instances in which Xerox copies of a former student's Ontario Secondary School Record Card(OSR-2) was sent to a university admission

officer by his high school principal in support of the former student's application for admission to university. This was done in contravention of the Ontario Secondary Schools Act. It is questionable whether all this information can profitably be used in helping the child and persuasive evidence that it can be used to discriminate against students perceived to be undesirable for social, cultural, or political reasons. Even the existing format appears to be insufficient to fulfil the requirements of some school districts. We found a school district in eastern Canada to be circulating a supplementary questionnaire asking the religious denomination of all students' families although prior questionnaires had already established whether the families were public or separate school supporters.

Secondary and primary school authorities tend to cooperate more closely with local police than do their counterparts at university. We cite the following instances of cooperation: a primary school teacher assisted in entrapment of a student on liquor offence charges; authorities at a secondary school helped direct a police search for narcotics in student lockers; a primary school principal permitted police interrogation of a student in an investigation of vandalism without first notifying his parents; a secondary school principal called in provincial police to be present when he admonished students regarding "tire squealing".

One school board's administrative service department provides computer processing for over 100,000 student records. The board has jurisdiction over more than a hundred public schools, more than two dozen junior high schools, nearly a score of secondary schools, and two vocational schools.

The basic record continues to be the traditional card folders used throughout the province. The manual records are stored and maintained in the schools. They follow students whenever they are transferred to other schools and no copies are retained at the former school. Records of graduates are stored at the school from which they graduated. Records are available to principals, vice-principals, counsellors, teachers, nurses, and school psychologists. In this district, the students or their guardians have the right to review the student's record card.

The school board computing centre performs grade reporting, scheduling, and enrolment for school principals. The students complete a basic data intake form, an update form, and a course selection form. Teachers complete grade report forms.

The data form contains basic information on the student, guardian, emergency contacts, and school standing -- a little over 200 characters in all. The contrast between the computer record and the traditional record card is striking. In fact, the increasing use of electronic data processing equipment in this province is one of the prime reasons that the design of the uniform school record card is currently being studied for radical revision for the first time in 50 years.

Student records are batch processed; a driver picks up and returns the forms to schools. Key punching is done at the computing centre. Grade reports are produced by the computer centre four times a year and issued by the schools. Individual scheduling reports are issued in the spring, enrolment reports in the fall. The school personnel are responsible for verifying information. No historical files are maintained in machine-sensible form.

In addition to processing student records the centre provides for processing the school district payroll, processing student programmes, test scoring, work order systems, inventory systems, and academic instruction. From a physical security point of view, the system is atrocious. As if mixing instruction with payroll and personnel records processing isn't bad enough, the centre itself affords minimal effective security from either physical threats or improper access to data. Security of records is not all that good either. Normally three generations of tapes are maintained with the grandfather stored off-site in a locked cabinet in one of the Board's secondary schools. The computing centre is located in the main administration building.

CHAPTER 9

POLICE INFORMATION SYSTEMS

The police are a professional paramilitary organization of sworn officers charged with enforcing the federal criminal code and relevant local and provincial statutes. As such, they are a part of the criminal justice system which includes also the courts, crown attornies, justice ministries, jails and penitentiaries, parole boards, and probation offices.

In the course of gathering material for this section, one member of the Task Force attended the International Security Conference in Chicago, Illinois, May 24 - 26, 1971. While there, he obtained a certificate in the course Investigation II, which covered: techniques for identification and recall, single fingerprint comparison, surveillance techniques, handwriting comparison, preparation for court and testifying, and crime scene search and preservation of evidence. Portions of the following section were reviewed for accuracy by Inspector Laverne Shipley who is in charge of training for the London Police Department. The Task Force extends its thanks to Chief Walter Johnson and the officers and men of his department for their cooperation in our study.

Basic Police Activities

There are six basic activities in police work. In order of their involvement of personnel, they are: patrolling, control, communications, investigation, identification, and intelligence. Records keeping will be dealt with later in this chapter. These six functions are by no means tightly compartmented and, in his daily work, the average officer moves easily from one to another.

Patrolling

Patrolling is the principal activity of a police force. Patrolling may be done on foot, in a motor vehicle, or from a fixed post. Its main purposes are showing presence, civilian contact, observation, and response.

The control function is often an adjunct to patrolling and may consist of crowd, traffic, or area control, such as may be implemented with road blocks.

Communications

Communications is the hallmark of a modern police force and its cohesive effect is what puts the "force" in police force. Radio, use of call boxes, and oral briefings are all types of communications. Reports are received from the patrol force (and

other police officers) which result in advisory notices, alarms, or directives. An advisory notice modifies an officer's actions on patrol. Examples are vacant property notices, stolen vehicle or licence plate lists, bogus currency warnings, and stolen property notices. An alarm indicates that some major occurrence has taken place and evokes action, which may entail area control; the action taken is usually in compliance with some prearranged plan. A directive creates an immediate response in reaction to an incident.

Reports are the principal product of police activity. Reports received from officers may be of a general nature describing various types of crimes or offences, supplementary to prior reports, or of a more specialized nature such as missing persons, homicide or sudden death, stolen or impounded motor vehicle, lost or found, fraudulent cheque, or accident. Reports which concern wanted persons, released criminals, or arrests may originate internally or with other police forces.

Reports from officers on patrol or more specialized duty arise from civilian contact (complaints about law breaking), observation, police action taken, such as the arrest of a person or the impounding of a vehicle, or from investigation.

Investigation

Investigation is the central activity of the detective branch of a police force but can involve uniformed officers also. In general it begins at the site of an occurrence -- accident or crime -- and involves basically the preservation of physical evidence and the questioning of witnesses or victims. A popular mystique surrounds physical evidence but its value is principally corroborative; few convictions are secured on the basis of tire and footware impressions, dust, soil or stain analysis, tool or rifling marks, or even latent partial fingerprints alone. Human testimony nearly always plays a key role; and to establish motivation, prior planning, and conspiracy, it is essential. If the day ever comes when the average citizen becomes unwilling to speak truthfully to police officers, our police forces would have to work under a crippling handicap.

Study of the occurrence site usually leads to search, seizure, and apprehension involving open areas, buildings, vehicles, persons, or property.

The interrogation of suspects is central to any police investigation. If guilt invariably had to be established beyond a reasonable doubt in adversary procedures, the criminal justice system would become hopelessly overloaded. Interrogation differs from questioning in that the police have the suspect in custody

and can control the time, place, and circumstances. An interrogation proceeds in cycles of breakthrough, expansion, and confirmation. The initial breakthrough or preliminary statement is of paramount importance. Getting a preliminary statement is not as hard as it sounds. Most criminals like to talk about their exploits; but, like all human beings, they need to rationalize their confessions. We can heavily discount tales of coercive police interrogation although a large man with a loud voice can be as persuasive in an interrogation room as he can on a used-car lot. Techniques vary with the circumstances and with the interrogator. Sometimes accusation of a more serious crime than that under investigation will induce the suspect to relate the details of his involvement. Sometimes the inference that an accomplice has confessed, or an equivocal suggestion of clemency, the actual or averred possession by the police of important physical evidence, or disclosure of the existence of an eye witness can lead to a breakthrough. Non-stop interrogation by relays of interrogators also is largely a myth although it may be necessary to go over a preliminary statement several times with a suspect before he can be induced to expand upon it; the suspect is usually induced to do so by pointing out inconsistencies among his repeated versions of his preliminary statement. The manner of the interrogator towards the suspect can vary from demanding, to austere, to a sympathetic attitude -- or a change of pace can be introduced as in the hawk/dove or "Mutt-and-Jeff"

approach. We hear little of the polygraph used as a stress detector; it is useful principally in pointing out areas of sensitivity where interrogators may wish to probe further.

Backgrounding is one field of investigation in which citizens with no other involvement may become ensnared in the criminal justice system. Essentially it consists of having the subject complete a detailed questionnaire on his prior life which is then checked against official records and by field investigation. A questionnaire will typically provide for identification of the subject, give name-change, citizenship, marital, employment, education, military and residence history; details on family members, in-laws, and foreign travel; and cite from three to five references. Documental checks of security questionnaires involve consulting criminal records, registries of births, marriages, and divorces, records of citizenship courts, passport applications, and military service records. Field investigation includes interviews with references, former employers, educators, and neighbours at present and former addresses. In some jurisdictions a credit check is also made using an in-file or investigative reporting agency. Few actual foreign agents have ever been unmasked by backgrounding, however. Professional agents usually fabricate legends with the typical background checks in mind. Thus one foreign agent appropriated the birth certificate of a deceased resident of Cobalt; and one case on the West Coast involved an individual accused of supplying a foreign

government with names and addresses of defunct companies and demolished residences to use in fabricating legends for illegal agents. When backgrounding does turn out useful it often results in impeaching the right people for the wrong reasons.

Identification

Identification deals with persons, motor vehicles, property, firearms, questioned documents, narcotics and dangerous drugs.

Most positive criminal identification today relies upon use of fingerprints. Fingerprint identification consists of two functions: classification and comparison. All 10 prints must be present for classification. Use of primary and secondary classifications results in defining some one million categories in which fingerprint records may be aggregated. Unfortunately some classifications are much more heavily populated than others. Thus other attributes of fingerprints must be sought to distinguish among persons. Single fingerprint comparison is especially useful in dealing with loops, the most common basic fingerprint pattern. Some police forces maintain single fingerprint files on break-and-enter men and auto thieves. In making a single fingerprint comparison, the analyst proceeds outward from the core (or centre) assigning each staple (or loop) a letter category defining peculiarities perceived in it. The number of points of similarity required for

positive identification is usually left to the judgment of the fingerprint technician. Modern dactyllography has been extended to include the study of the prints of the papillary ridges of palms, toes and the balls and heels of feet as well as the patterns of skin pores on these ridges.

Physicial identification in Canada still relies principally on hair, eye and skin colour, height, weight, facial hair, and hair style although all these are now subject to easy and often spectacular change or camouflage. Modern physical identification tends to concentrate on eyelids, eyebrows, lips, face shape and, to a lesser extent, noses and ear lobes. (According to a system developed by Deputy J.A. Cormack of the Sawyer County (Wisc.) Sheriff's Office). There are a few cases on record in the States where voice prints (sound spectrometer tracings) have been used to identify suspects, especially in cases relating to threatening phone calls. This service is offered commercially by Voiceprint Laboratories Corp. of Somerville, N.J.

Identification of motor vehicles and personal property such as firearms, tools, appliances, stock certificates, and currency is facilitated by serial numbering in addition to such obvious attributes as manufacturer or issuer, colour, and description. Interior ballistics including the study of marks left by the firing pin and extractor on cartridge cases, and rifling marks on bullets

is useful in firearms identification. Licence plates and, in some jurisdictions, title, are applicable in identification of motor vehicles. In some jurisdictions files of laundry marks (one system was developed by Inspector Adam Yulch of the Nassau County (N.Y.) Police Department) are maintained to aid in identification of clothing; as are jeweller's or watchmaker's marks for identification of jewellery and watches. The type of questioned document most frequently dealt with is the fraudulent cheque. In such cases handwriting and habituation in respect of setting forth the amount of the cheque are useful points of identification. (The letter is the basis of a cheque classification scheme developed by the late Ralph Bradford of the Long Beach (Calif.) Police Department). The handwritten letters F, T, and Y are particularly useful in identifying handwriting. The recognition of narcotics and dangerous drugs can be aided by comparison with simulated samples made from synthetic materials and available in kit form. Positive identification, however, requires laboratory analysis.

Intelligence

Police intelligence is a subject about which officers are understandably reluctant to talk and consequently this leads to wide ranging speculation and perhaps even fear on the part of civilians. Basically most police intelligence is obtained from informers. It has been said that a detective is only as good as his sources of

information. Although the use of paid police informers may not be unknown, such sources are relatively rare and not always productive from a cost/effectiveness point of view. Useful information is more likely to be gathered from more casual contacts, observations of alert citizens, interviews with parolees and probationers, and as a by-product of specific interrogation or questioning. Casual contacts may include those made with probation with parole officers, welfare workers, and insurance investigators. Cases of tax fraud, welfare fraud, credit-card fraud, insurance fraud, shoplifting, defrauding inn keepers, pilferage, and vandalism frequently entail close co-operation and information exchange with private security officers and officials of government agencies nominally outside the criminal justice system.

Surveillance is another word with unpleasant connotations to many civilians but the plain facts are that surveillance is expensive and time-consuming. So-called "fishing" expeditions consequently are rare and surveillance, as a whole, tends to be productive only when used to confirm information previously obtained by other means. Surveillance divides into two areas: visual and technical. Visual surveillance may be mobile or conducted from fixed posts. The distinction between visual and technical surveillance is becoming less clear than formerly inasmuch as technical equipment such as binoculars, spotting telescopes, infrared viewers, and directive microphones may be used to augment visual

observation, while equipment such as cameras and audio or video tape recorders may be used to record the events observed. Use of two-way mirrors in interrogation rooms and closed-circuit television cameras in detention cells are forms of visual surveillance. Mail cover, or the recording of cover (envelope) notations on mail addressed to a particular location has found considerable favour in some jursidictions but seems to be little used in Canada. The principal forms of police surveillance consist of following suspects, checking out registry books in some places of transient accommodation and passenger lists of aircraft, and staking out probable crime scenes -- all of which require considerable prior information and typically occur in the late stages of an investigation. Technical surveillance refers particularly to use of equipment for wiretapping and eavesdropping. The use of radio locating equipment to keep a target vehicle under surveillance is really an extension of visual surveillance using highly sophisticated technical equipment. Technical equipment used for wiretapping and eavesdropping may rely on either wire or radio to transmit signals from the point of interception to a location where they can be recorded or evaluated. Equipment used may or may not include facilities for recording intercepted conversations. It usually does.

Wiretapping attacks are aimed at telecommunications lines -- commonly telephone lines. The point of attack may be anywhere along the line from the telephone instrument to the central office but it usually is at some intermediate junction box. The technique of eavesdropping attacks enclosed spaces in which suspects may engage in incriminating conversation. Typical spaces include offices, hotel and motel bedrooms, residences, and motor vehicles. Radio transmitters may be concealed upon undercover operators or informers to monitor their activities and frequently to safeguard their lives. Wiretapping is most useful in securing evidence against criminals whose activities are carried out necessarily with the use of telephones -- bookmakers, extortionists, and stock "boiler-shop" operators. Eavesdropping is used principally in establishing cases of criminal conspiracy. Agents with hidden wireless microphones are effective in narcotics cases and in establishing cases of attempted bribery of public officials. Generally speaking, a great deal of preliminary work is necessary before technical surveillance can be employed productively. Its principal value is in confirming intelligence derived from informers.

Undercover operations provide an endless source of fascination or apprehension to civilians. In general, they consist of use of decoys, enticement, infiltration, and, in the continental European context, provocation. Use of decoys, especially where a bureau of policewomen exists, can produce useful results in cases

of mugging and molestation. Enticement is a prime tool of morality squad officers and often serves to allow drug pushers to incriminate themselves. Infiltrating police officers into criminal conspiracies is difficult and not often accomplished successfully but the police should take no onus from the fact that their officers do not readily pass muster as members of the criminal element. Provocation is not a tactic that has gained favour in Canada. It perhaps reached its nadir in the days of the Tsarist Okhrana when a police agent provocateur actually engineered the assassination of the Minister of the Interior.

Future Challenges

There are three principal challenges that face the police in the last quarter of this century. They are suppressing organized crime, controlling revolutionary activism, and coping with advanced technology. The three are not unrelated. Organized crime, more properly syndicated crime, is characterized by accumulation of capital usually by unlawful methods to finance further criminal endeavour. These capital resources in turn make advanced technology available to the criminal, for example, the thermit lance and technical surveillance equipment. At the same time, police intelligence gained through technical surveillance is necessary to strike at the principal unlawful sources of income for syndicated crime, for example, bookmaking.

Revolutionary activism leads to criminal activities on the part of persons who would not otherwise have come to the attention of the police. They may be much better educated than the traditional criminal and frequently travel in circles where sources of police intelligence are scarce. In dealing with revolutionary activists, police can expect modern technological developments to be turned against them, for example, some of the ingenious homemade bombs recently encountered in the United States. Also, there remains the need for a socio-political long-range warning system to provide information about incipient trouble. This may require creation of information systems beyond the traditional police pattern. Development of these systems will probably require a total community effort and little if any of the activity involved is likely to be of a clandestine nature.

Challenge of technology is three-fold; to use it to advantage, not to be overwhelmed by it, and not have it used against the police. The last facet was commented on in connection with syndicated crime: it should be added that computer-aided embezzlement may become an area of some concern. Few police organizations have used the computer to its fullest effectiveness, of course the same can be said for banks, insurance companies, and even universities which have an experience with computers that is of much longer standing. Potentially the collection and analysis of incident statistics can lead to more effective patterns of patrol activity,

area control, and general resource allocation, and the amalgamation of the computer and the police communications system can lead to faster and more effective response. However, there is a very real danger that unthinking expansion of a computerized communications system can produce a debilitating information overload on the part of police officers, permit leaks of information that can be damaging both to the personal reputations of individuals under investigation and to police effectiveness, and leave the police organization vulnerable to criminal attacks on its communications channels.

POLICE

(Site Interviews)

Task Force studies relating to police information systems entailed visits to the Solicitor General's Department to meet representatives of the Royal Canadian Mounted Police, Canadian Penitentiaries Service, and National Parole Board, and the Records and Inquiry Branch of the Toronto Metropolitan Police.

In these and subsequent sections dealing with government information systems, we do not feel it is within our area of competence to generalize, abstract, or interpolate. Consequently, in the remainder of this report we will tend to rely heavily upon information adduced during site interviews and to take the statements made by government officials at face value in the absence of factual evidence to the contrary.

SOLICITOR-GENERAL'S DEPARTMENT

The Solicitor-General's Department is responsible for the RCMP, the Canadian Penitentiaries Service, and the National Parole Board. It was formed in 1966. As of September 1970, 65 persons were employed at the Solicitor-General's Headquarters. The Department utilizes electronic data processing in Personnel and Financial reporting systems for management and research. It utilizes computers controlled by the Department of Labour, the Department of Supply and Services (Computer Services Bureau), and the Public Service Commission.

In the operational context, or where the Department is undertaking its own research, data security measures depend upon the nature of the computer service involved. If this is government operated, for example, the Computer Service Bureau, no particular measures are taken as it is understood that the organization would operate within the ambit of governmental security provisions.

However, if a bureau from the private sector is involved, personnel from the Solicitor-General's Department would be on hand to ensure that all punch-cards etc. are returned after the operation.

If the Department is having research conducted for it by universities etc., the contract involved contains a clause whereby information about individuals or likely to lead to the identification of individuals will not be made public.

ROYAL CANADIAN MOUNTED POLICE

The RCMP has the responsibility of policing 23% of Canada, on a population basis. It divides its files into administrative files: those concerned with files on its own personnel and internal management; and operational files: criminal records and security and intelligence.

The Criminal Record file is currently held in manual form. The record is derived from the Fingerprint Section or FPS file, when fingerprints (on criminal charges) are submitted to the Identification Branch. The present file of one million individuals with criminal records has accumulated over the past 60 years. Each record consists of a fingerprint card cross linked to a photo, if available, and a record sheet carrying the FPS number, date and details of each sentence, place of conviction, charges, disposition, name and identification of the officer contributing the item. Note local police records (the principal input to the FPS) may include also the items: nationality and occupation, in some cases physical identification, modus operandi (MO), and criminal associates. Records of pardoned criminals are kept in a separate part of the FPS file. Records are not made in the case of summary or juvenile convictions (according to provincial laws defining these categories). The governing principle is whether fingerprints are taken or not. When a suspect is charged with an indictable offence and subsequently

discharged, his record is expunged only if he requests return of his fingerprints. Records are kept until the criminal dies (this must be confirmed by fingerprints submitted by a police agency) or until the criminal attains the age of 70 and has been out of trouble for five consecutive years. Fingerprints taken by the military do not become part of the FPS file.

The most significant development in RCMP records keeping will be the Canadian Police Information Centre (CPIC). The system, to become operable in 1975, will cost $36 million over six fiscal years. It will be built around an IBM360/65 to be installed in 1972 in a new $3.3 million building between RCMP headquarters at 1200 Alta Vista Drive and the Rideau River. The CPIC system currently employs 100 persons; 300 will eventually be employed. Annual cost will be $5 million. The central computer will have 1 million bytes of core; also disk and tape drives. It will be linked with 10 provincial RCMP headquarters over private dedicated lines to be leased from common carriers. No additional safeguards are being proposed at this time to protect against wiretapping. Investigation in this regard, however, is continuing. RCMP headquarters at Vancouver, Edmonton, Regina, Winnipeg, Toronto, Ottawa, Montreal, and Halifax will each have one Interdata model 14 computer (a mini-computer to be used as a message concentrator) establishing synchronous communications with Ottawa. Each headquarters will also have two Interdata model 13 computers, each capable of handling

16 asynchronous inputs from KSR 33 or 35 teletypes. The system will connect with 250 police departments (Police Act forces only) in this manner. Communications will be in the half-duplex mode. Main-trunk communications will be established over 4800 baud lines. Other lines will operate at data rates of 2400, 1200, 300 or 110 baud. An advisory committee will set policy regarding access, confidentiality and security. Member forces of this co-operative police network will determine the allocation of terminals within their own commands.

The CPIC will handle four disk files kept both in English and French: outstanding warrants, stolen vehicles, stolen property, and criminal records. Users will be able to access all files on-line. They will update the first three files on-line although data will be accumulated on tape and checked against the file before update in-place is undertaken. Contributions to the criminal record file will be batch processed. A journal tape of all updates will be maintained. The criminal record file will be backed up with hard copy, photographs, and fingerprint cards. Local police forces will be able to "bank" data, such as summary offence matters and local (30-mile) warrants outstanding, for their exclusive use. The manual system contains 1 million records. The CPIC system may or may not contain this number; no decision has been reached as to whether all these records will be automated; CPIC will also be used to process RCMP administrative data.

Under the present manual system, police forces throughout Canada maintain their own comprehensive record systems. With the implementation of CPIC, there would be no necessity to retain or build up their filing systems as it would be more expedient and advantageous to utilize the CPIC data bank.

The wanted criminal file will contain data on outstanding warrants validated every 30 days.

The stolen vehicle file will contain licence numbers, make, year, colour, serial number, body type, and physical description e.g. "bashed in rear fender". There is no facility to search on partial licence numbers.

The stolen property file will be set up on type of article and subclass (type, make, and serial number in the case of firearms).

The criminal record will be of variable length. It will include name, FPS number, penitentiary number, fingerprint classification, charge sheet information, and criminal associates, if available. However, the system study of the criminal record file has not yet been completed.

Basically, the CPIC relies on physical security of the terminal and exercise of command responsibility over users. Terminals are identified by "here is" transmissions. The computer

will recognize only legitimate terminals on the CPIC system, therefore, it is believed that unauthorized terminals being introduced into the network would be immediately detected. Use of passwords and read/write authority codes has not yet been decided upon. There is no provision for use of privacy transformations. An audit trail of user accesses will be facilitated by a tape record, which will store terminal number and message.

It is planned to extend the CPIC system in the following ways: add stolen stock certificates to the property file, provide for real-time processing of administrative data, computerize the files regarding registration of handguns, and computerize the S & I files. Real-time transmission of video data is at least five years away.

Release: 1) Subpoena power extends to criminal records on an individual not class basis (e.g. one cannot get a list of "all bank robbers"), 2) sealing records of pardoned criminals does not guarantee that local records will be erased, 3) communication with foreign police forces is conducted on a manual basis, i.e. mail or teletype. This includes communications with the FBI and the 105 national police forces that are members of Interpol. The most frequent interchange of information with the FBI is by teletype regarding stolen vehicles. Commissioner Higgitt told the Globe and Mail on July 8, 1970 that "maybe 20 or 30 cases a day pass between (the RCMP) and the FBI. Maybe 15 letters a day."

During our interview with representatives of the RCMP the subject of Security and Intelligence (S & I) files was raised. The RCMP representatives confirmed that 1) S & I files exist, 2) they are not at present in machine-sensible form, and 3) they may at some future time become computerized. Beyond that, no further information was communicated. A brief description of U.S. practices regarding the handling of internal security information appears at the end of this section.

CANADIAN PENITENTIARIES SERVICE

The Canadian Penitentiaries Service holds 7400 committed persons (as compared with 14,000 in provincial jails). Its records include files on its own personnel, housekeeping files, inmate records, stock control, and accounting files for prison industries. Electronic data processing is also a rehabilitation activity for inmates.

An inmate record includes a face sheet, FPS record, medical record, and instititutional history. It includes a case history (classification report) and a psychological report. It may include the results of a psychiatric examination. Inmate files are held in hard copy form at the institution where the inmate is held, at the Central Registry at the Canadian Penitentiaries Service Headquarters, and in computerized form at the headquarters of the Solicitor-General's Department. The EDP files are processed at

CSB, where they could be vulnerable to potential intrusion by centre personnel. Inmate records are considered to be confidential and non-producible, the Service has refused to confirm, in divorce actions, that a spouse is indeed incarcerated or to release to spouses an inmate's destination or address while on leave. Records can be released to officials of the Penitentiaries Service, National Parole Board and the Solicitor-General's Department. The RCMP is notified of escapes and releases. The RCMP furnishes the FPS record upon receipt of a newly admitted inmate's fingerprints, which are used to confirm his identity.

Cooperation from reformatories and provincial jails is generally quite good and information is provided to them upon request from federal institutions. In Ontario, the federal receiving institution sends requests for information on every inmate previously incarcerated in a provincial institution and information is willingly provided. A high degree of cooperation also exists in British Columbia. Some federal institutions elsewhere make only occasional requests from the provincial systems. Provincial systems make much fewer requests for information from the Penitentiaries Service, presumably because they have had these inmates on prior occasion and possess adequate information. When they do make a request, the Service provides the information.

No breakdown of the contents of the computerized record is available. Presumably this is face sheet data which characteristically includes: name, date-of-birth, marital status and history, ethnic origin, years in Canada, religion, details of sentencing (court, place, adjudicator, charge, arresting officer), bonding, restitution, summary of prior criminal record, educational history, employment history, home conditions, details regarding parents and spouse, summary of medical, psychological, and psychiatric examinations, organizations of which the inmate is a member, hobbies and interests, clergy references, and persons and agencies interested in the case.

The Penitentiaries Service does not use the same guidelines as the RCMP with regard to purging inmate files of the records of deceased or pardoned criminals. If an inmate dies while serving a sentence, his file is destroyed. If he dies after release, his file is kept for three years and sent to archives where it is kept and where it is destroyed on the day on which has expired a period of five years after he has been released from a penitentiary.

The file of an ex-inmate who has reached age 70 and has had no offence in the previous five years is destroyed. In cases of life sentences, whether the inmate is deceased or not, the files are kept indefinitely at archives. The files of pardoned inmates are dealt with in the same manner as any ordinary inmate file, kept three years, sent to archives and destroyed.

Penitentiary personnel are bound by the Public Service oath of office to keep information regarding inmates secret.

Institutional standing orders state that inmate files are confidential and officers shall not discuss inmates or ex-inmates with unauthorized persons if it will affect the administration, discipline, or security of the institution. Access to inmate files is limited to senior staff: warden, deputy warden, assistant deputy warden, classification staff, National Parole Board, recognized social agencies, psychologists, and psychiatrists. All other officers or persons outside of the Penitentiaries Service requiring information must consult the Deputy Warden, Assistant Deputy Warden, or the Classification Officer.

Penitentiaries Service regulations make all members responsible for the confidentiality of inmate records. Commissioner's policy directives provide guidelines in connection with the use of Claim of Privilege in dealing with applications for the production of confidential information in legal proceedings, advise all personnel of their duty and responsibility regarding the confidentiality of inmate records, and direct Classification Officers to give those officers not authorized to use inmate files the information necessary for their work.

The Warden and Assistant Warden are the only officers authorized to pass information regarding the operation of the institution or an inmate or ex-inmate to communications media.

When inmate files are kept in the inmate training area, only senior institutional management have free access to them. Other officers must refer requests to the Classification Department which provides the specific information needed, using professional judgment as to what to release. For example, while a vocational instructor might need to know the occupational background and attitudes of an inmate, he would not need to know that he has had extramarital relationships.

Data concerning inmates including professional reports are released only to official organizations in the process of helping their rehabilitation. Professional records, medical and dental, are communicated only to hospitals and the like on a need-to-know basis.

NATIONAL PAROLE BOARD

The National Parole Board maintains manual files on all inmates of federal correctional institutions since all are subject by law to automatic parole review, and those inmates of provincial institutions who actually apply for national parole.

Data is extracted from these files along two dimensions. First, data is collected regarding the nature of the decisions of the Parole Board in exercising its discretion under the Parole Act. Secondly, data is collected on the personal characteristics of the offenders about whom such decisions were made. In the latter instance, the offender population is divided, for each calendar year, into three main categories: those for whom parole was denied, those released on parole, and those whose parole terminated and why.

Usage of the data is currently twofold. The first is to publish a set of tabulations showing significant cross-classifications between the variables. The second is to plan the data on tape as input to a relatively flexible programme that will enable other cross-classifications to be realized on specific demand.

With regard to the handling of parole records by Statistics Canada: it is understood that under the provisions of the Statistics Act all employees of Statistics Canada are required to take an oath of secrecy relating to material and information that becomes known to them in the course of their duties and that this provision covers, in a general sense, the needs of the existing parole system.

At the same time, in particularly sensitive cases that are well known to the public, it has been seen necessary to non-report certain data fields such as destination.

A reporting programme to monitor the administration of the Criminal Records Act is now under development and follows the same lines as that indicated for parole. It remains to be decided who will provide the EDP processing medium. The proposed programme provides for code numbers to be assigned to cases rather than utilizing the person's name, and a manual linkage, which will be restricted, will be maintained between the two.

Pardons granted by the Governor General, which are not subject to revocation, do not represent input into any reporting system. A local manual count is maintained by Clemency and Legal Division of the National Parole Service.

SECURITY PLANNING AND RESEARCH GROUP

Since the visit of the Task Force to the Solicitor General's Department a new group was formed on August 28, 1971. It is the Security Planning and Research Group; at its inception it had three members: Col. Robin Bourne, a former advisor on internal security to the Privy Council and an artillery officer, Lt. Col. Walter Dabros, a former member of the armed forces security branch, and S/Sgt. Patrick Banning, formerly of the RCMP; it will probably develop to include 20 persons.

Described as a clearing house for information, it will advise the Cabinet and federal government on threats to national social, political, and economic order. It will have no direct connection with other police forces but will have close ties with the RCMP and other forces. It will not carry out investigations into espionage or assume other duties performed by the RCMP's security and intelligence branch.

TORONTO METROPOLITAN POLICE

Most of the files kept by the Toronto Metropolitan Police are manual ones. Metro will hook up experimentally with CPIC in October 1971; probably for input and challenge by the Records Bureau; and for challenge only by the station duty officer at all five districts.

The principal files kept by the Records and Inquiry Bureau are: Central Index, Complainant & Victim File, Accident File, Stolen Property Description File, Serial Identifiable Property File, Stolen Car File, Personnel Files (internal), Summary Conviction Records, and Arrest File.

Gun Records are kept by Departmental Support Services; Juvenile Contact Records by the Youth Bureau; and Criminal Records by the Identification Bureau.

The Central Index contains one million 3x5 cards in eight elevator-type tub files. The index is alphabetical by individual's name. Each entry contains name, address, file reference (colour coded), and description: age, height, weight, hair and eye colour. Entry data is received by telephone and the index cards which are created as a result of the telephone conversation are compared later with an official report. Nine classes of subject individual are included in the index:

1) Wanted persons -- initiated by General or Local Warrants, Bench Warrants, and Committal Warrants.

2) Missing Persons -- 10,540 last year, the card is initiated by a Missing Person Report, a Telex goes out also.

3) Criminal Records -- the index card directs one to the Criminal Records File.

4) Summary Conviction Records -- the index card directs one to the Summary Conviction Records.

5) Suspensions -- lists are supplied by the Ontario Department of Transport.

6) Interdicted List -- lists are supplied by the Liquor Control Board of Ontario.

7) Probationers -- information is supplied by the courts.

8) Parolees -- information is supplied by the National Parole Board.

9) Juvenile Contact Cards -- index cards direct one to the records held by the Youth Bureau.

The following summary traces a hypothetical history of an individual's involvement with the Central Index: based upon an occurrence report, a warrant is issued for his arrest and a card goes into the index; when he is apprehended, a card goes into the Arrest Record File (recording name, age, address, and date-of-birth) and the warrant card is removed (the arrest card remains one year in the arrest file, another year in the vault); if he is convicted, a criminal record or summary conviction record card goes into the index; these cards are removed in case of a successful appeal or the granting of a pardon.

The Complainant and Victim File consists of 200,000 colour-coded 2 x 1 1/4 in. tabs arranged alphabetically by last name of complainant or victim and keyed to occurrence reports filed separately.

These occurrence reports include:

1) General Occurrence Report
2) Supplementary Report
3) Fraudulent Cheque Offence Report
4) Bicycle and Tricycle Occurrence
5) Motor Vehicle Occurrence
6) Impounded or Held Vehicle Report
7) Missing Person Report
8) Lost or Found Report
9) Homicide and Sudden Death Report
10) Record of Arrest

There are 146,000 offences against the criminal code filed annually and 43,000 provincial code offences (mostly drinking). Police officers submit reports on 4-part forms. One copy is retained at the district station. Reports are filed by type of crime and name of complainant. Crime reports are kept seven years; lost or found reports three to four years.

Stolen Car Reports are put on the computer and a "hot" car list printed out weekly and distributed to all divisions. Stolen car reports are checked against abandoned car report information. Cars are listed by licence and serial number.

Stolen property index consists of a description: type of appliance or tool, colour, manufacturer etc,; this file is kept on punch cards.

Crime statistics: type of crime, place, and date are computerized.

Records of Serial Identifiable Property are kept in a manual file. Police information on stolen property may be released to the victim for insurance or customs purposes.

The Accident File (35,500 per year) is ordered by persons involved, date, and place. All accidents are recorded irrespective of cost: Police will release information regarding a specific accident to insurance companies on request. Accident records are retained five years.

Gun records are filed by serial number and name; permits both to keep and to carry firearms are filed.

Criminal Records consist of photos, fingerprint card, and record of convictions. Records are not released but information from them is typed for release. This information is releasable to accredited police departments and courts for pre-sentence reports. Lawyers can obtain information from their client's records. Local police officers request information through their divisional inspector or detective sergeant i/c. Records are filed by the CIB (Criminal Identification Bureau). Clerks are sworn to secrecy under penalty of dismissal. In the event of successful appeal, dismissal or withdrawal of charges, or pardon, records are destroyed, or the charge is marked off if more than one charge appears on the record. Records are kept until proof of death is received.

Summary Conviction Records are kept separately (RIB). They contain neither photos nor fingerprints. Access provisions are same as for Criminal Records. There are 10 cabinets; individual records range from one to ten or more cards in length.

Personnel Records. Records on 4,000 active personnel and former personnel are kept in jackets and on CFAX cards. It is planned to microfilm these records. Records consist of 20-30 pages. There is a system of annual personnel evaluation. Evaluations are superceded in three years. Employees must ask to see their own

files through their unit commander. Offfcers in charge, the complaint bureau and staff counsellors are permitted to see records. Files are retained indefinitely. Consent of the individual is necessary before any information -- even address and phone number -- is released outside the department.

U.S. POLICE INFORMATION SYSTEMS

A few words should be said about U.S. developments in law enforcement information systems, since developments south of the border, rightly or wrongly, often provide a pattern for Canadian systems evolving subsequently.

However, there are several basic points of difference between U.S. and Canadian law enforcement systems which must be understood first.

1) At the federal level, all law enforcement responsibility in Canada devolves upon the RCMP. In the U.S. every department of the federal government has its own enforcement branch; some departments have several such branches.

2) In Canada, the functions of law enforcement and criminal prosecution are separated at the federal level, being assigned respectively to the Solicitor-General's Department and the Department of Justice; in the U.S. they fall within a single department (the Department of Justice).

3) In Canada there are few examples of overlapping police jurisdiction and all police (except CN and CP Railroad Police) are enforcement arms of some level of government: federal, provincial, or municipal. In the U.S., there may be several police forces operating at different and overlapping levels of government; and many quasi-governmental "authorities" have their own police. Thus they have park police, throughway police, housing police, bridge and tunnel police, sanitation police, transit police, public buildings police, fire police, etc.

4) In Canada private investigators and security guards are just that and nothing more. In the U.S., many private police obtain legitimation as peace officers by various devices, for example, by having them appointed "special deputy sheriffs".

5) In Canada, there is one criminal code. In the U.S., there are 50 state criminal codes as well as a federal criminal code and the definition of a specific crime is by no means uniform among state codes. These state codes do not correspond to provincial by-laws; they cover most common-law indictable offences (called "felonies" in U.S. parlance).

6) In Canada, an individual becomes "criminal" only upon conviction for an indictable offence, at which time he is fingerprinted and his record sent to the Fingerprint Section, Identification Branch of the RCMP. In the U.S., all justice "transactions" may become matters of record somewhere. The concept of what constitutes a "transaction" is by no means uniform but usually includes any arrest. There is no clear distinction between transactions based upon the allegation of an indictable offence and a summary offence ("misdemeanor" in U.S. parlance). There seems to be a great deal of local discretion involved in deciding which records are forwarded to the FBI and which are retained locally.

There are four major developments in the formulation of computerized criminal justice records systems.

1) The NCIC or National Crime Information Centre has been operated by the Federal Bureau of Investigation since 1967. It is based upon on-line files located in Washington, D.C. The files deal with wanted persons and stolen property, especially motor vehicles and firearms. There are 40,000 police jurisdictions that could tie into NCIC; only 4,000 have so far.

The FBI's National Crime Information Centre is a computerized information storage and retrieval system now containing over three million records.

The NCIC files contain information on wanted persons and stolen or missing property which can be identified by serial number. This includes firearms (more than 421,000 lost or stolen guns including those reported missing by private citizens and all military arms missing and not declared battle loses), vehicles, boats, licence plates, other serially identifiable articles, and negotiable securities.

The computer for the NCIC is located in Washington, D.C. Terminals are located in each state, usually at State Police Headquarters; some large municipal and county police departments have terminals as well as does the RCMP Headquarters in Ottawa.

FBI field headquarters have terminals as do several federal agencies such as the Army, Navy, Marine Corps, and Air Force investigative branches and the Secret Service. As of November 1971, 45 of the 104 terminals were fully computerized so that data is keyed directly into the computer in Washington without having to pass through any human intermediate operator. The data fed into the computer is stored immediately so that information can be extracted in three to five seconds after it has been filed.

The NCIC began operations in January 1967 with only 16 law enforcement agencies on-line with the computer and a base file of 23,000 records. Five years later, it handles more than three times that each day -- about 75,000 transactions, including

information placed on file and inquiries. About 750-800 "hits" per day result. In the gun section alone a recent check revealed an average of 366 reports per day of lost, stolen, or recovered firearms, and more than 1,400 inquiries per day. No figures are available on the number of "hits" per day in the firearms section (The American Rifleman, January 1972).

2) Various state police systems of which the NYSIIS (New York State Identification and Intelligence System) is best known. Not much is known about the state of implementation of these systems nor about their scope; which is likely to vary widely from state to state. We have in hand the initial proposal for the NYSIIS and it calls for an exhaustive dossier on each subject including details on personal habits and associates. However, we understand that system implementation has fallen short of what was initially proposed; various trade-offs have been made with regard to what information would be computerized, what information would be held in manual form and what information could not be collated into compatible form for all records. It is known that when implementation was undertaken, some 30% of the manual records that were to provide input were found to be in error.

3) Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories) is a cooperative venture by 15 states financed by the federal Law Enforcement Assistance Administration (LEAA), an instrumentality of the Department of

Justice. The system conceives of the maintenance of state-held criminal history files and a central index directly accessible by each state. The central index will respond to inquiries by furnishing the following information:

1) personal descriptions: *name; *sex; *race; place of birth; *date of birth; *height; weight; hair colour; skin tone; visible scars, marks, tattoos, amputations, or deformaties; miscellaneous identifying numbers; *state ID number; *FBI number; social security number; operator's licence number; and fingerprint classification;

2) an abbreviated criminal profile;

3) the name of the state or agency holding the full criminal history (Agency of Record).

When a criminal justice transaction takes place between an offender and an agency in a state other than the Agency of Record, the file is transferred; the file is updated; and the central index is updated to reflect these changes.

---

* The starred elements are the minimum required for entry of a record in the central index.

A test was conducted in July-August 1971. A file of 100,000 records was placed on-line using a Burroughs B-5500 computer belonging to the Michigan State Police. Seven states were on-line with the system using telephone lines: Arizona, California, Florida, Maryland, Michigan, Minnesota, and New York. Connecticut had inquiry-only access via New York's computer.

Evaluation of the test is incomplete and observers disagree as to its degree of success. However, as a result of preliminary findings, the federal Department of Justice has directed the FBI to operate a national criminal history exchange through the NCIC. The Service to be provided by the FBI will consist of the basic central index utilized in Project SEARCH.

4) Various criminal justice monitoring systems one of which is functioning in the municipal courts of Los Angeles. Another, called Project TRACE is under development for Washington, D.C. These systems deal with cases referred to courts for adjudication and have for their objective the expediting of cases through the criminal justice process.

INTERNAL SECURITY

It would be useful to comment on the way in which the U.S. makes use of personalized records in internal security operations. This is difficult, however, because of the incredible complexity of the U.S. security and intelligence establishment and the widespread duplication of duties among agencies.

We may consider, however, what transpires when a U.S. citizen applies for a position which requires security clearance. In such a situation, the applicant completes a Personal History Statement not unlike that used in Canada. He delivers it to his prospective employer's security officer who may have him photographed and fingerprinted, often using the firm's own facilities. The material developed is forwarded to the security officer of the procurement agency with which the firm has contracted.

Depending upon the level of security clearance required by the position for which the applicant has applied, a National Agency Check alone or in conjunction with a Full Field Investigation will be ordered. The National Agency Check consists of consulting the files of the Federal Bureau of Investigation; Army, Navy, and Air Force Intelligence Commands; the Subversive Activities Control Board (formerly the House Unamerican Activities Committee); and in some cases the Atomic Energy Commission Intelligence Division.

When a Full Field Investigation is required, the National Agency Check is supplemented by having investigators verify the statements made by the applicant in his Personal History Statement. The investigators who do this verification are employed or retained by the military service with whom the firm has contracted.

Internal security is a mission delegated to the Federal Bureau of Investigation. Few confirmed facts are available as to how the Bureau discharges its responsibilities. It is believed that Special Agents assigned to internal security duties work out of regular Bureau Field Offices and report through the same chain of command as do Special Agents assigned to criminal investigation. It is known that Special Agents cultivate and pay informers within organizations suspected or engaging in subversive activities. Persons, alleged to be Special Agents of the FBI, have been reported as having been observed photographing participants in protest marches and infiltrating protest groups in a variety of disguises. However, because of the duplication of effort in U.S. internal security operations, it is difficult to say with certainty for just what agency these observers were, in fact, working. We do not know exactly how the FBI files are organized and what portions of these files are consulted during a National Agency Check. There is reason to believe, however, that fingerprint comparisons are not always made to verify identity since sometimes clearance is granted without fingerprints having been submitted. The affirmative response to a National Agency Check is "nothing derogatory."

The intelligence commands of the Army, Navy, and Air Force now feed their information upward to the Defense Intelligence Agency, an instrumentality of the Department of Defence. Prior to 1971, personalized information assembled by the armed services intelligence commands had been centralized in a computerized national Security Data Bank at Fort Holabird, Maryland. When controversy regarding this data bank developed in the Senate of the United States, the Department of Defense announced that the National Security Data Bank had been abolished and its data tapes wiped. However, it is believed that the files were merely returned in machine-sensible form to the agencies that had originally contributed them.

The operations and organizational details of the intelligence commands of the three service arms are all different but there are some essential similarities. Because of recent publicity regarding its surveillance of certain politically motivated organizations, we have chosen to discuss in this report the activities of the Army Intelligence Command. Since we are interested only in activities within the context of internal security, the missions of the Army Security Agency (radio interception) and the Army Map Service will not be of consequence here. The Army Intelligence Command is a staff activity. (It was formerly called G-2, the second section of the Army General Staff). Its strategic function, which includes supervision of Military Attaches, is concerned with

collection of information regarding the land warfare capabilities and intentions of foreign nations. However, it is the Army's capability for collection of tactical intelligence which is most relevant to the question of internal security. Tactical intelligence organizations (S-2) exist within all Army units -- regular Army, Army Reserve, and National Guard -- down to the battalion level. There also exist specialized units -- regular and reserve -- trained in tactical intelligence, Counter Intelligence Corps units, and units of the Criminal Investigation Division of the Corps of Military Police. To these, as potential gatherers of internal security data, should be added the Emergency Ordnance Disposal units of the Ordnance Department.

When the Continental Army commands and the subordinate Corps area and Military District commands began to perceive certain revolutionary activists as potential internal enemies after troops had been used several times for riot duty, it was natural for these commands to utilize their existing tactical intelligence organizations to gather personalized data concerning these individuals. It should be noted that within the Continental Army Commands, military intelligence personnel have often been supplemented by civil service investigators and private investigators retained on contract. In addition it has been a practice to issue "appropriate duty" orders to certain reserve intelligence officers and enlisted specialists enabling them to earn "drill pay" by following certain

individuals or infiltrating organizations as directed by local commanders. By utilizing these resources, the U.S. Army was able to assemble voluminuous files concerning individuals suspected of engaging in subversive activities. Eventually these practices came to light when some former Army investigators gave testimony before a committee of the U.S. Congress with the result that the Army came in for some sharp criticism. It is not known to what extent this criticism has modified the U.S. Army's information gathering practices. It is believed that in Canada all persons gathering personalized information relating to internal security matters channel their findings to RCMP officers assigned to Security and Intelligence duties.

Another file of consequence containing internal security information in the U.S.A. consists of the names of persons who have made threats against the President or other high government officials or have demanded personal interviews with them. This file is maintained by the U.S. Secret Service, an agency of the Treasury Department which has among other responsibilities that of protecting the persons of the President, Vice-President and their families. Persons whose names appear on this file have been known to have been placed under extremely close surveillance during presidential visits to locations near where they live. It is not known whether or not this particular file has been computerized.

CHAPTER 10

MOTOR VEHICLES

Motor vehicle registration and operator licencing are provincial matters. Rising concern over the increasing frequency and severity of highway accidents is leading to the maintenance of more detailed records on drivers. Most provinces have a point or demerit system whereby drivers can lose their right to drive by persistent violations of the applicable provincial highway traffic act. The driver who earns a suspension of his driving privilege nearly always feels his privacy has been invaded; the relatives of persons killed by reckless or drunken drivers always feel that the driver responsible should have had his privacy invaded a great deal sooner.

In most provinces, some kind of insurance is required to obtain a licence or to register a vehicle. As premium charges are usually related to the principal operator's driving record, some sort of dossier system obtains here to.

Automobile negligence suits are one of the principal sources of court activity and in turn give employment to hoards of insurance adjustors, claims investigators, private detectives, damage appraisers, and forensic physicians. All this legal activity leads to a lively traffic in accident reports, driving record transcripts, and various other items of documentation.

We visited one motor vehicles documentation agency, the Motor Vehicles Branch of the Manitoba Department of Transport. In several ways, Manitoba has pioneered many advances in motor vehicle and operator documentation. In general, the Province of Manitoba seems to put more stock in objective assessment rather than the socio-economic predictors frequently used elsewhere by private insurance carriers. On the other hand, Manitoba tends to deal more severely with the chronic violator and physically incompetent driver.

MANITOBA MOTOR VEHICLES BRANCH

The Manitoba Motor Vehicle Branch (MVB) files are particularly interesting because of the recent introduction of provincial auto insurance.

The files consist of the driver's licence file, the vehicle file, the truck file, and the snowmobile file. In addition, certificate files are kept by the Motor Transport Board on public service vehicles (vehicles which haul the goods of others) and commercial trucks (vehicles which haul the owner's own goods in trade without area restrictions). The certificate files contain terms and conditions of operation such as areas and type of goods.

There are four recognized types of trucking operations. Straight (ordinary) trucks having a "T" licence plate are authorized to carry any type of goods within a radius of 10 miles of greater Winnipeg, or within 15 miles of any other community in Manitoba.

Farm trucks are permitted to carry the farmer's produce or goods for use on his farm only. The farmer is absolutely prohibited from hauling for hire.

Commercial trucks so registered permit the owner to transport his own goods only to any part of the province or to another province. He cannot transport any other person's goods for compensation.

Public service vehicles are carriers licenced currently by the Motor Transport Board, and shortly to be licenced by the federal Canada Transport Commission in the case of extra-provincial carriers, which are authorized to transport goods or passengers for compensation.

Ordinary truck and farm truck records are maintained with the passenger vehicle records (that is, on computer). It has been proposed that commercial truck records be incorporated in the file along with the records of ordinary trucks, farm trucks, and passenger vehicles; this may happen during 1972.

The driver's licence file consists of 440,000 records held on random-access disk. Three generations of tape are kept as back up, also a COM-produced microfilm file (computer-output-to-microfilm). Backup storage facilities are maintained in an on-site vault. Records are stored on all drivers who hold or have held licences within the past five years. Criminal offence records are held on microfilm for a period of 10 years.

A Driver's Licence record consists of the following information: name, address, date-of-birth (DOB), sex, licence number (five letters of surname, initials, DOB and tie-breaking numbers -- computer produced), convictions (Manitoba has had a penalty demerit system since 1951; points are erased by good driving if other conditions such as retesting, which may include road, medical, or optometric tests, are met), accidents (including blame indication), actions of MVB subsequent to an incident (warning, interview, suspension), status of licence, conditions (are restrictions, types of vehicle for which valid, "bread & butter" permit), restrictions (hand controls, corrective lenses), insurance (no-fault insurance), results and date of driving test, medical report (if required -- a medical report is mandatory for drivers over age 65 or if the applicant indicates he has had a disabling condition).

Dissemination of driver's licence records is as follows: 1) MVB main office; 2) the RCMP will have its own terminal (juvenile convictions -- under age 18 unless adjudicated by an adult court -- and MVB actions are blocked out); 3) other Police must phone or write for data (St. James, St. Boniface, Winnipeg, and RCMP have copies of the microfilm file); 4) insurance companies (can request status, personal identifiers, accidents and convictions only; MVB actions subsequent to incidents are not reproduced -- the report issued is called a transcript of driving record); 5) credit bureau (when requested, the MVB will verify the validity of licence, driver name and address); 6) employer (a transcript will be issued with the written consent of the driver); 7) interprovincial and U.S. exchange (MVB send transcripts on request; it sends notification of convictions to the offender's home jurisdiction; only criminal conviction of non-residents are entered on the Manitoba file; MVB sends the surrendered licences of newcomers to Manitoba to their former jurisdictions and requests transcripts); 8) physicians from whom a medical opinion is requested (transcript); 9) attorneys (client's transcript).

Hard copies of driving record transcripts are not court admissible unless signed by the Registrar of Motor Vehicles and the Deputy Minister of the Department of Transport. Note that the Provincial Insurance (Crown) Corp. is manpowered by law to pursue government records, the provisions of the Manitoba Privacy Act notwithstanding.

Inputs: A birth certificate must be presented to obtain a driver's licence; a five-year two-part licence is planned with photograph of the driver. No inputs are received directly from provincial Medicare but doctors may report patients having disabling conditions; the doctors are protected legally from action by the patient for breach of confidence; only eight or nine such reports were received from doctors in the initial period from September-June 1971; it is planned to make this reporting mandatory in the future. Psychiatric hospitals at Brandon, Selkirk and Winnipeg send to MVB the names and reason for admission of new patients who possess drivers licences (MVB then requests a medical report). The Blind Institute and Pension report their new clients who have drivers licences to MVB. When complaints about individual drivers are received, a warning letter and a call for interview are issued if the driver has no record of prior convictions. If complaint is with regard to alcoholism, a medical report is obtained and reviewed by the MVB medical advisor -- police may investigate discreetly. If the driver complained about has a record of convictions, the complaint is usually referred to the police for investigation.

No-fault insurance attaches to the driver; basic premiums are: male over 25, $7; female over 25, $3; male under 25, $22; female under 25, $7. Premium increases to $50 when six penalty demerits are assessed and upwards to a maximum of $300 if the maximum number of points is accumulated.

The existing unsatisfied judgment act will continue in force until 1974-5. Note that drivers resident in Manitoba for less than 90 days do not have to register with MVB; and that the provincial insurance plan act does not cover hit-runs. There are no plans now to investigate insurance applicants beyond acquiring information regarding them from other government files.

The vehicle file contains 420,000 160-character records; it is currently held on tape but will be put on random-access disk in July (1971). It is updated weekly; three generations of tape are kept in on-site vault storage; COM microfilm records are used as backup and supplied to police. A vehicle record includes: name (of owner), address, age of vehicle, make, style, model, serial number, and public liability insurance (currently carrier name or whether a $25 contribution has been made to the provincial unsatisfied judgment fund; after November 1971 the record will show whether the driver carries basic or supplementary provincial insurance). It is planned to add colour of vehicle (the owner will have 15 days to advise of change of colour of the vehicle), area of operation, number of cylinders, use (business or pleasure), and DOB of owner. It is felt that because of the advent of provincial insurance it will become necessary to link drivers licences with vehicle registrations. It is planned to institute a motor vehicle title law both as an anti-theft safeguard and as a means for lien registration. Currently only a bill of sale is required to register

a motor vehicle. There are plans to institute a surcharge to the owners of motor vehicles which have been involved in accidents. Present AUTOPAC insurance is $250 deductible collision (the deductible amount can be lowered to $100 or $50) and $50,000 public liability (can be raised to $300,000); both the government and private firms will sell supplementary insurance.

Information is sold to the public from the vehicle file as follows: a) given a plate number (or name and address) a requester can obtain name and address (or plate number), cost 50¢; b) same with a detailed description of the vehicle, $1; c) mailing lists of car owners at 10¢ per name (these lists were formerly sold to R.L. Polk at 1¢ per name). It is noted that rules regarding car ownership by welfare recipients have been relaxed.

The snowmobile file contains 18,000 records. It is currently held on tape, but will be placed on random-access disk. All snowmobiles south of 53^{0} N latitude (south of 55^{0} in towns) are registered for three years for $15. The same data are collected as in the case of passenger motor vehicles. It is planned to collect data on cubic-centimeter engine displacement as this information may be utilized to determine future insurance cost. No microfilm records are produced.

The truck file is kept manually. It contains data on commercial trucks and public service vehicles.

Documentary files are kept on convictions (three months after acquisition these data are microfilmed), notices of suspension, accident reports (kept for one year and afterwards microfilmed), medical, and optometric reports.

Data processing is carried out on a IBM 360/50 computer belonging to the province. The computer is shared with Taxation, Education, Municipal Affairs (assessment), Highways, Public Works and legal statutes.

MVB has one systems analyst, 2 programmers, 16 keypunchers, and 11 terminal operators. The data processing group performs methods and systems studies, data entry, display and input/output control. Several control measures are in effect: a record of point deletions (removal of demerits from a driver's record) is printed out and checked manually.

Files are updated by punched cards but other methods such as terminal update, use of a remote card reader, and use of keytape are under consideration.

Formerly MVB got printouts from the computer file twice a year with addenda every 2 weeks; now microfilm is supplied twice a year with weekly printed updates. Five cathode-ray-tube (CRT) terminals and two 2740's are linked by phone line to the computer system. The RCMP has five CRT terminals to the system. At

the MVB head office a one-time password is used to open the system each day (18 hr of shift operation but terminals are locked at end of the MVB working day). Five persons have the code of the day which is passed from the computer as part of the sign-off message; there is no additional means of user identification.

Displays at MVB are used in checking applications, reviewing complaints relative to assessment of penalty points, producing transcripts, completing reports of convictions, and collating accident reports and convictions with drivers licences (the computer is used to match up various permutations of the driver's name).

CHATTEL MORTGAGE REGISTRATION

The Personal Property Security Registration System under control of the Ontario Department of Justice will be integrated with the system by which the Department of Transport keeps track of vehicle registrations and drivers' licences on its IBM 360/40 computer and perhaps with other departments of the provincial government.

The system will keep track of conditional sale contracts for $300 or more on consumer goods, chattel mortgages and the assignment of book debts by companies. Some 300,000 loans are currently registered each year at 48 county and district offices

(for $1 anybody can search these manual files). The average loan is for $3000. About 80% of all conditional sale contracts signed in Ontario are signed by people buying cars on time. Almost 80% of all chattel mortgages are signed by people borrowing money from banks or credit unions to buy cars.

Persons querying the system will phone an information centre in Toronto which will interrogate the computer while the caller waits; cost will be $2 an inquiry. The system went into effect on January 1, 1971; the existing manual record-keeping system will be phased out by 1974.

CHAPTER 11

TAXATION

A psychiatrist from Clarke Institute of Psychiatry in Toronto told us an anecdote about one of his patients who was receiving psychotherapy for an assortment of sexual deviations. After a session in which he described many of his episodes, the psychiatrist asked him a question about his income: "None of your business", replied the patient, "that's private information".

We all seem to regard information about income as private information but we must lose this part of our privacy to the tax man. However, unless we want to give up our self-assessment principle and return to earlier more brutal and less efficient forms of tax gathering, this is a part of our privacy we have to surrender because of an overriding social concern. However, if information given to the tax man is used for purposes other than raising revenue, the picture changes.

The Task Force confined its study of taxation systems to a visit to the Department of National Revenue-Taxation, and to a leading income tax consulting firm.

DEPARTMENT OF NATIONAL REVENUE - TAXATION

The Department of National Revenue-Taxation has the responsibility for collecting federal individual and corporate income taxes, estate tax and old age security tax. It collects provincial income tax for all provinces except Quebec; it collects Canada Pension Plan contributions for the Department of National Health and Welfare; and, as of January 1, 1972, it will collect unemployment insurance. It is based in Ottawa and does business through seven regional centres and twenty-nine District Taxation offices.

Eight computerized files contain data which might become personally identifiable: (1) the TAPMA or master file of individual taxpayers (10,500,000 records, 500 characters each); (2) the CINDAC or individual accounting and collection file, i.e. receivable (600,000 to 1,500,000 records, 400 characters); (3) PAYDAC or employer source deduction file (500,000 records, 300 characters); (4) MAT-4 or T-4 supplementary data file (15,000,000 records, 40 characters); (5) green-book - a 6% statistical sampling file -- name/address removed (500,000 records, 400 characters); (6) list of corporations (250,000 records, 100 characters); (7) taxation personnel file (12,000 records, 100 characters); and (8) historical file (9,750,000 records, 400 characters). All files are kept on 9-channel magnetic tape (125 reels for TAPMA file) in three generations, one in a tape vault, and one in an off-site vault.

Data are processed on an IBM 360/65 computer in the batch mode; 234 employees are engaged in data processing supplemented by 1,000 temporary keypunch operators at peak load periods. The Department has two other computers: an IBM 1401 and an IBM 7074.

Tax returns, principally the T-1, are filed centrally. The majority of the returns are associated with the taxpayer record by social insurance number. This number is obtained either from the label on the direct mailed personalized returns or in many cases from the number quoted by the taxpayer himself. Returns without any social insurance number are associated by taxpayer number, a combination of alphabetic and date-of-birth data. When this information is not available, the returns are sent back to the District Office for manual reference.

Returns are scanned manually at the time money is taken for deposit from the tax-return envelope. In the manual pre-audit procedure, totals are run of attached T-4 slips against reported earnings, and the totals of attached receipts from charitable institutions are run against claimed deductions.

Selected data are keypunched to create the historical file, which is the basis of the TAPMA file. Returns are then checked arithmetically and by certain "obvious" build-in logic checks.

Confidentiality is maintained in the keypunch area by having the alphabetic and numeric keypunching carried out by different units. The volume of production makes it virtually impossible for the operators to read anything other than that which they are keypunching, or in fact to remember any of it at all.

Also, the returns for each keypunch operator to work on are selected by the unit head. Returns awaiting processing are handled by the unit head. This means that individual operators cannot see any returns that are not given to them for keypunching and they have no opportunity to select the returns they do receive. The oath of office and secrecy is given to all staff, either permanent or temporary. There is no ironclad guarantee that staff will not divulge information that they encounter in their work. The best the Department can do is to hire prudently, minimize opportunities, and maintain a high level of close supervision.

Hard copy returns are returned for storage at district offices. Audits are performed on a statistically selected base sent to each district. Presumably hard copy stored at the District Office, as well as records in Ottawa, are covered by the confidentiality provision of the Income Tax Act:

> "Every person who, while employed in the service of Her Majesty, has communicated or caused to be communicated to a person not legally entitled thereto any information obtained under this Act or has allowed any such

person to inspect or have access to any written statement furnished under this Act is guilty of an offence and liable on summary conviction to a fine not exceeding $1000.00."

The final check of an individual return is a post-audit done by running the MAT-4 against the TAPMA file. Except for 125 largest employers who submit a total of 2,000,000 records already on magnetic tape, the employer's supplementary T-4 return is retyped in regional centres and converted to tape on rented optical scanners in Ottawa. The MAT-4 or T-4 supplementary file totals are checked against employer payments reported on the PAYDAC or employer source deduction file.

We have no real knowledge about the confidentiality provisions with respect to employers as regards employees' T-4 slips. We do know that the T-4 slips are required by some social-welfare benefit administrators in connection with means testing.

INFORMATION OUTPUTS

1) The Dominion Statistician has access to corporate tax returns to enforce the Corporation and Labour Unions Returns Act (1965).

2) The Statistics Act of 1971, permits the Dominion Statistician to examine statistically selected samples of individuals' returns. He has access to information according to arrangements agreed to

by the Ministers of the two departments. This means the Department of National Revenue-Taxation cannot be forced to abrogate its own standards of confidentiality.

3) Information required to prosecute tax fraud cases is supplied to Crown Attorneys. Information about a taxpayer's return is given to law enforcement once it has been decided to prosecute that taxpayer under the Act.

4) Tapes are sent to nine provinces on their own taxpayers. Quebec handles its own tax records; thus its tax records can be used in means testing and verifying statements of income made in support of applications for student awards -- officials say this saves the province $6 million a year in grants denied to ineligible applicants who might otherwise have received awards. In the other provinces, in spite of the tax tapes having been returned, the province cannot use the information on them for any purposes other than statistical ones since the confidentiality operative at the federal level extends to these nine provinces as well.

5) Although the normal TAPMA or taxpayer master file is ordered on taxpayer account number (first five alphabetical characters of the taxpayer's surname, his Julian date-of-birth, a three-digit file sequence or tie-breaking number, and a check digit), an extract is made of 60% of this file. It consists of

the names of taxpayers whose principal income is from wages. This extract of the TAPMA file is ordered on taxpayer Social Insurance Number. It is then checked against the MAT-4 or T-4 supplementary file to verify the proper reporting of income tax withholding information and is also utilized to supply information on payments to the Canada Pension Plan to the Department of National Health and Welfare.

6) The supervisor of the Tax Roll Section must authorize requests to see files. A taxpayer may see his own return at the District Office but no protocols have been established for access to hard copy of returns held at the District Office with regard to the taxpayer himself.

7) Batched T-4 slips on U.S. residents are sent to the U.S. Internal Revenue Service; and IRS sends batched W-2's (a U.S. IRS document comparable to a T-4) to National Revenue-Taxation, in accordance with treaty obligations.

8) Information from the list of corporations is linked to Statistics Canada data bases.

9) Green book statistics describe taxpayers in aggregate. (3-5 taxpayers minimum in any published category).

FUTURE PLANS

1) Computerizing T-4A's (investment income) and T-5's (interest payments).

2) Computerizing T-2's (corporate returns). The list of corporations was compiled as a step in this direction.

3) Provision for remote enquiry to a central data base from District Taxation Offices over common-carrier lines.

SECURITY

Principal security measures are concerned with internal auditing and preserving the integrity of computer spaces. The Department is also concerned with preserving the integrity of all file storage areas, whether for tape files or hard copy. Vandalism in general including bombing is seen as the only threat to security over which the Department may not have as high a degree of control as it would wish.

INCOME TAX CONSULTANTS

Between January 1 and June 1 of each year Canada's taxpayers need help. They turn to income tax consultants. One of the largest (H. & R. Block) regards itself as a division of a U.S. parent company. Its director of Canadian operations is based in the U.S. state of Kansas.

During the rush period, the firm expands from a skeleton force of 100 to some 2,000 staff and from one to two offices per city to 287 offices, some of which are franchise operations.

About 1/4 million Canadians avail themselves of this firm's service. Each customer's file consists of a copy of his tax return and any related correspondence. Files are kept five years. During the peak season files are kept at the office with which the customer deals. During the off season, files are kept at the manager's office for that city. There is no central nor back-up file but a complete list of customer names and addresses is sent to the head office in Kansas.

A company representative told us they do not often receive inquiries about customers and it is company policy not to give out any inforamtion from customer files.

However, recently a large finance company approached most offices of H. & R. Block with a proposition. If these offices would furnish a list of all customers owing taxes above the amount withheld, and all customers expecting a refund, the finance company would pay the informants a percentage of the profit made lending money to customers in debt to the tax man. We were told that all offices in Canada refused to go along with this scheme. There is some question, however, as to whether some of the company's U.S. offices did participate with this finance company or with other groups seeking to obtain information about customers. The issue became the subject of legal proceedings in the U.S.

The Canadian branch admits to mailing out one sales promotional letter a year telling its former customers it is tax time once again. Customer files are used if required by the client for tax audit purposes.

An interesting aspect of the tax advising business is that the advisors do not seem to feel they are dealing in information of a highly confidential nature. And, according to them, neither do their customers.

This particular company is not computerized. Although they have tried computers, they have decided against continued use of them on economic grounds.

CHAPTER 12

CENSUS

The Dominion Bureau of Statistics is unique among information gathering agencies in that individuals and business organizations have a legal obligation to furnish information to it and, in turn, it has a legal obligation to maintain the privacy of individual statistical returns. Note that subsequent to our visit the name of DBS was changed to Statistics Canada.

The principal activity of DBS in terms of people involvement is the Census of Population, taken every 5 years (more extensive data is collected at 10 year intervals). Two forms were used in 1971, Short (2A) and Long (2B - given to 1/3 of subjects). The Census of Agriculture is taken at the same time. Enumerators distribute forms; they keep visitation records with forms identified by household number to facilitate follow-up. (Questionnaires may be picked up or mailed in. If a subject decides the enumerator is personally unacceptable to him, DBS will send a census commissioner or a full-time DBS agent). Mailed-in questionnaires are delivered to the enumerator concerned for a check for completeness and to see if all questionnaires delivered have been returned. The forms are also checked by the field office and the head office. The most sensitive questions appear to be those dealing with income.

Several U.S. Bureau of Census employees, duly sworn in under the Statistics Act, accompanied enumerators in a field test of the Population Census in St. Catharines; Canadian DBS men have also participated in the U.S. tests.

Two microfilm records are made of each form: 1) FOSDIC records (computer sensible microfilm) for computer entry -- no names or addresses and 2) census search records. Forms are destroyed by shredding after microfilms are made (about two years). Census search files are sometimes consulted on behalf of individuals trying to establish facts relating to their own age or residence at some time in the past and to draw DBS post-censal sample surveys.

The FOSDIC images are read and converted to magnetic tape. The computer edits the data, checking for inconsistencies. The backup of the tape records during computer processing consists for about two years of the original forms.

The data processing staff at DBS numbers 300; there are also 150 programmers. Activities include programming, systems analysis and data processing. Data entry, for non-census work, generally is accomplished by key punching, key edit (agricultural census) and document OCR, as well as FOSDIC (for population census). DBS has an IBM 360/65 with 1 million bytes of core, 20 disk units, and 17 tape units; also an IBM 1401. Some computer processing is done outside DBS -- mostly for development of computer programs.

If personally identifiable data is to be processed, DBS employees transport the data, remain present during its processing and swear in outsiders engaged in the processing.

In addition to handling the population census, DBS carries out a great many other studies. Among other fields it has a responsibility for the collection of judicial statistics -- paroles, pardons, convictions. It also has special privilege to obtain income tax information. It is hoped to use these personal income tax data between censuses although tax data have some limitations on two counts; they are 1) incomplete (all residents don't have to pay tax) and 2) reported on an individual, not household basis. A survey of household incomes is conducted annually over a sample of 10,000 - 25,000. Employment statistics, which constitutes an important economic indicator, are published each month in conjunction with Canada Manpower and released at a predesignated time; they are based on a sample of about 35,000 households. In compiling business manufacturing statistics the central list, a numbering of companies for DBS internal use, is employed: the identifying numbers include industry classifications and geographical codes. Lists are published which identify companies by name, address, industry, and employee groups.

DBS publishes population information in the form of statistically aggregated data. Lowest geographical level released for the census is the enumeration area (except, possibly, counts of people by city block). The lowest geographic level for data release is determined independently for each survey in such a way as to ensure confidentiality.

DBS will furnish information about a subject (respondent) to another government department only if the subject (usually a business) so requests. (Such a request may be made to avoid filling out a second questionnaire).

Under the 1971 Statistics Act, information furnished to DBS by another government agency retains the confidentiality classifcation given it by the collecting agency.

Release of aggregate information in the form of data banks is a recent development. It is stressed, however, that no national data bank of identifiable individual returns is planned. CANSIM (Canadian Socio-Economic Information Management System) exists as a data bank of publishable (aggregate) economic time series. It would be operated on-line only if detached from DBS computers processing personally identifiable data: use of non-identifiable census data in connection with simulation experiments appears to be possible under the new Statistics Act.

The GRSDR system (Geographical coding of data for retrieval) was discussed. Individual census data are coded to block faces (urban) and enumeration areas (rural). DBS furnishes data for geographical areas defined by the user, those areas can be smaller than enumeration areas but must be greater than block faces. Several hypothetical situations were discussed in which a user might attempt to "play games" with the system to obtain identifiable data. A few of these can be categorized as follows: 1) small-sample disclosure 2) incremental disclosure and 3) residual disclosure. Various measures can be taken to counter such attempts and a fully automatic procedure has been designed as part of GRSDR to ensure the statistical confidentiality of the resulting tabulations.

To this list of problems, we have tentatively added another, which might be called "agency disclosure". It takes place, for example, in a university context, when DBS requires a breakdown of the student population or faculty by nationality and immigration status. On the surface, this appears to consitute no invasion of individual privacy inasmuch as only aggregate data are requested. However, to be assured of an accurate count, the reporting institution often feels it has to associate each response with a named individual for check-off purposes. In this way, the individual's personal information becomes known to the reporting institution although not, of course, to DBS. In some cases, the

institution would normally have collected these data in any event, so the reporting to DBS in no way creates any additional invasion of privacy. However, in some cases, the institution would not have collected these data save for the DBS requirement for reporting statistical aggregates. In fact, in some provinces, the institution might have been forbidden to collect such data inasmuch as their possession by the institution could provide the basis for unlawful discrimination against the individual. Such conflicts arise in other instances such as where a provincial human rights code forbids discrimination on the grounds of, say, nationality, and then a federal regulation is promulgated which, for good reason, does in fact discriminate against persons on the grounds of nationality; for example, excluding persons on student visas from receiving certain federal research grant funds. The problem of "agency disclosure" poses a dilemma but is by no means insoluable. Imaginative data collection procedures could facilitate collection of accurate statistical data without individual linkage, and specially designed storage facilities could permit discrimination against individuals where required while protecting their privacy where that is required.

The problem of traceability arises in the handling of statistical aggregate data although possibly not in the immediate context of DBS operations. Suppose one conducts a study at a given point in time and breaks the population of interest into groups,

say, drug users and non-users. It may later be of interest to cross classify these groups at some subsequent point in time by some other attributes, say, in gaol or at liberty. It is of no interest to the researcher to have these data personally identifiable but they must be linked for traceability. One technique for doing this is to use a scramble tape; associate each case entry with a random number which is keyed to identity data only on a separate tape. The case history data identified and eventually linked by only the random numbers can be made generally available for study, while the key tape is preserved under conditions of utmost secrecy and wiped after linkages are made. In one U.S. study of youth attitudes regarding drug use etc. the key tape has been stored in Canada to insure against its being subpoened by the American courts.

The Committee of Presidents of Universities of Ontario is considering use of a similar security system to preserve individual privacy in a proposed data bank of Ontario university students where a major point of interest will be delineating the migration of students among universities within the province and discovering correlates of such movement such as the students' marks, local economic opportunity, course offerings, etc.

The final problem raised in our visit to DBS concerned the situation in which the personal data of a potentially sensitive nature (e.g., birthplaces of criminals) is collected to dispel popular misconceptions. The point being that although collection of such data may constitute some invasion of individuals' privacy there is a more valuable social purpose served by obtaining statistical evidence that, popular works of fiction notwithstanding, only a small proportion of persons of Italian origin become involved in criminal activity and that this proportion compares favourably with that of other nations.

Statistics Canada concedes that the quality of its enumerators and other part-time census personnel is a continuing problem from the point of view of confidentiality of respondent information but that the relatively low pay available, the large number of personnel involved, and the highly intermittant nature of the work make it impossible to achieve any satisfactory remedy.

CHAPTER 13

TELEPHONE

Canada's telephone companies are major users of computerized information systems. By numbers involved, their directories are the largest lists of personalized information in the country. Few people, however, consider that a telephone directory listing constitutes an invasion of privacy. This is not true in other countries, however. In the Soviet Union, no telephone directories are published and a potential caller must be given a number by the subscriber. This practice is put forward as an example of the preservation of individual privacy in the U.S.S.R., although there is suspicion that the practice may be motivated more by considerations relating to state security.

More importantly, perhaps, the telephone companies maintain the lines over which computer teleprocessing data flow and the security of these lines thus becomes a point of paramount concern to all users of remotely accessed computing facilities.

With regard to customer (subscriber) accounts, the basic intake forms from which records are developed by telephone companies are the application and contract cards completed by customers. Besides basic personal identifiers and the type of service desired, the company obtains information on the occupation

and salary of the would-be subscriber and the name and address of a friend or relative -- the former set of information is taken for credit evaluations; the latter as a means for contacting the customer when he cannot be reached at his listed address. It also provides a clue to trace him in the event that he later skips with a telephone bill owing.

Telephone companies have their own credit granting procedures. If credit bureaus are used, it is usually only with commercial accounts; these credit bureau checks are made with file-based reporting agencies. In cases of seriously delinquent accounts, the subscriber's credit information and the past-due account are turned over to a collection agency. Some telephone companies keep unpaid bills indefinitely; at least one company keeps all customer bill stubs for periods of from four months to one year, the latter period applying to accounts with which collection problems have been encountered. The record of equipment installed is maintained until the subscriber's account is paid or until a maximum period of six years has elapsed; the length of time the record is retained depends upon the size of the balance owing. Electronic-data-processing (EDP) files on former customers are kept four months. Credit records are kept indefinitely.

Telephone companies send billing information on collect calls to the called exchange, and exchange credit information with each other on a quid pro quo basis. The critical question appears to be whether a potential customer has telephone bills outstanding at the time he applies for new service. A credit information file is held on cards at district offices in telephone number order. In the case of questionable credit risks, companies require an advance deposit. Service may be refused to customers who owe money to a telephone company or to those who make abnormal requests for service which appear to be linked to illegal operations. The credit checking system works surprisingly well. We learned of the case of a young woman in eastern Canada whose husband was accustomed to run up large long distance toll charges. Eventually the couple separated leaving a large unpaid telephone bill. The woman returned to her parents home in another city. Within a short while her father was required by the telephone company to post a deposit of $100 to insure her good behaviour with respect to long-distance calling while living in his house.

Service and equipment (S & E) files are of interest because they contain information that might be useful to potential wiretappers. These files are presently kept in manual form at local commercial offices. One large telephone company is planning to consolidate and computerize its customer credit and S and E files; the file will be updated daily in the local batch mode and hard

copy printout distributed to local offices to update their manual files. The principal input to the S & E file is the assignment record which contains information which would be of interest to potential wiretappers. This information, including address, terminal location, cable and pair numbers, is kept by the plant department. Preservation of its integrity is the responsibility of the plant assignment centre foreman. The plant department maintains a list of customers by telephone number linked to cable number for purposes of maintenance and service. These data could help a potential wiretapper discover the locations of junction boxes at which to attack his victim's telephone line. Frame connection identification is kept at the central office and is the responsibility of the central office foreman. This information would be useful to a potential wiretapper intending to attack his victim's telephone line within the local central office. On the subject of line assignments, it is well to say a word about direct lines since these are frequently mentioned as being utilized in teleprocessing. Within a contiguous area, the term may mean a truly direct metallic connection that does not go through the switched network whose electrical characteristics can be measured and adjusted to suit the customer. Direct lines exist primarily for convenience and because of their superior electrical characteristics; the fact that a line is dedicated has no relevance to the problem of security of telecommunications. In fact, since the junction terminals of

these lines are identified by red plastic sleeves placed over the lugs to prevent tampering which might alter their electrical characteristics, they are, if anything, easier for a potential wiretapper to identify.

Collection of customer billing information concerning long-distance calls is becoming highly automated. Customer billing files in some companies are held as punched cards; other companies have converted them to magnetic tape. The files are processed by computer. The basic input comes from punched tape produced by automatic message accounting (AMA) equipment which records called number, calling number, and time of call. At least or company destroys the punched paper tape after three months. Toll records can be seized on warrant. Customer billing files are updated daily. Where AMA equipment is not in use operator produced toll tickets, usually mark-sense cards, provide the basic billing input. Records of operator assisted calls are recorded in cards; the name of the terminator is recorded for collect calls. These records are retained on microfilm, by at least one company, for three to six months.

In some areas the automatic equipment records only the called number and time of call; the operator must intervene to obtain the calling number. When mistakes are made in passing data at this point in time, telephone companies have been known later to charge the call to some likely subscriber who has often been known to call the city called in the questioned call or who just makes a large number of long-distance calls. Since AMA equipment does not function within a toll-free calling area, a pen register must be bridged across a line if it

is desired to make a continuous record of calls made by some subscriber who is the target of surveillance.

Toll fraud investigation is pursued vigourously by telephone company security departments. In one case we learned of a babysitter who called her boyfriend in a nearby city and improperly failed to report the call to her employer. This subscriber complained about the charge and a telephone security department investigator phoned the called number demanding to interrogate each member of the family until she had ascertained who had received the questioned call.

Customer data are used to compile directories, which may be published by an outside company. Customer data are used also for internal marketing and research analysis. Names and addresses are not made available for mailing lists or other commercial purposes in any form other than the directory. New directory listings are available only to intercept and information operators. Centrex lists, numbers for direct inward dialing, are available only from the customer himself. Names associated with numbers, except for unpublished numbers, can be obtained from the local business office.

There are three kinds of primary invasion of privacy that can occur in telecommunications lines: listening in by telephone company employees in the line of duty, surveillance by official police, or interception by private parties, with or without the connivance of subverted telephone company employees. It used to be the practice of telephone companies to listen in to portions of telephone calls selected on a random sampling basis (very small sample). The practice was called "service observing." It was done to determine whether operators were

handling calls properly. The practice came in for some considerable criticism in the U.S.A. during senate hearings by a committee chaired by former Senator Edward Long of Missouri; it was claimed that service observing constituted an invasion of subscriber privacy. As a consequence, U.S. telephone companies have stated that they have discontinued the practice. Although service observing never became a matter of public controversy in Canada, it appears that Canadian telephone companies have followed the lead of their U.S. counterparts. In our visit to Bell Canada, we noted that there is much less operator monitoring or "service observing" than there used to be although monitor-board positions still exist. The plant department records times of receipt of calls reporting trouble on a line.

Three terminal identification schemes are available to teleprocessing users; these schemes afford varying degrees of security; in one of these, the ASCII "here is" code character transmitted by the called terminal triggers a response from the calling terminal which consists of its transmitting a mechanically stored identifying message to the called terminal; the "answer back" provision locks out the calling terminal until the called terminal can check password files and establish communications; the "dial back" provision breaks off communication and requires the called terminal to call back on the calling terminal's listed number.

Telephone company security departments have five areas of responsibility: pre-employment checking of new male employees; investigating complaints of wiretapping and illegal use of telecommunications lines; internal investigation into improper conduct on the part of employees; surveying buildings to ensure that there is adequate protection, which includes protecting frame rooms, relay stations, and computer centres; and investigating unlawful acts directed against the company such as cases of toll fraud and coin-box theft. Security department officers generally have law enforcement backgrounds and may also have had craft experience. They check new employees for conviction records through law enforcement agencies and also check their driving records. Although ex-convicts may be hired for non-sensitive jobs, the company carefully screens its people, especially those who will work in vulnerable areas. One company reports that only 1/3 of job applicants are interviewed in depth, the rest receive only a brief interview, only 7% are hired. There is a 90-day probationary period which permits additional checking. This company shreds the application materials of unsuccessful applicants three months after the date the application was filed. When employees leave the firm, records are retained in an off-staff file for three years after which selected portions are micro-filmed. Subsequently the hard-copy files are sealed and stored in a central records facility.

Telephone operators and linemen are routinely checked upon to ensure compliance with company rules. Security men may also check on employees who handle sensitive company information, new subscriber lists, and unpublished numbers. Medical services report non-medical use of drugs to the Security Department and security men investigate these cases. The companies will discharge an employee if they feel his use of drugs is adversely affecting his job performance or if non-medical use of drugs is discovered during his 90-day probationary period.

The British Columbia Telephone Co., serving half a million customers, told us it gets an average of 10 complaints of wiretaps a month and that taps are found in about 10% of these cases. In addition, taps may be discovered as part of routine maintenance by linemen.

Complaints of wiretapping are handled by the Security Department. They are first referred to the Repair Service, which conducts a physical inspection of the customer's lines. If devices are found, they are deactivated and reported back to Security. The Security Department attempts to find out who is responsible for the tap. If it is discovered that the wiretapping involves a police matter, the police department responsible will be told to remove the equipment; presumably this will no longer be true when and if the proposed federal wiretap legislation is proclaimed. If the

police do not admit to the tap, the company may wait for the owner to contact them; security men will conduct a deterrent-type interview with the owner of the wiretap equipment before returning it. Presumably this procedure too will change if new legislation is proclaimed but as wiretapping is not yet illegal, no further action is now taken. Customers who are victims or targets of wiretapping are issued negative reports even if a tap is found.

The company co-operates with police in the investigation of illegal betting operations, prostitution, and drug trafficking. Telephone security men in Canada are just becoming aware of the potentialities of computer fraud. When information concerning numbers, listings and addresses or long-distance toll records are required for court purposes, a subpoena is required. The companies do not knowingly permit wiretapping nor making wiretapping facilities available to police departments. However, in the case of serious crimes such as kidnapping or murder, certain assistance is given to the police where it is felt that the public interest will not suffer.

Cases involving obscene and threatening telephone calls are investigated and attempts are made to trace calls in the most serious cases. Obscene phone calls cannot be traced unless the caller persists in making repeated calls or remains on the line for a relatively long period of time. About 100 traces are made a month by one company serving 1/2 million customers; the company

reports a 30% success rate. If the originator of routine nuisance calls is found, he is brought in and warned by telephone company security men. The second time, the caller's phone may be disconnected. If the customer insists, the caller may be prosecuted. Obscene calls may, upon investigation, result in prosecution. Security officers keep their files three years. They are then sent to central records and destroyed after 10 years.

British Columbia Telephone Company officials told us that the company welcomes federal wiretap legislation such as was introduced by the Minister of Justice in 1971 as it would provide a more effective means for controlling the problem than the present ad hoc measures. Most telephone men appear to be awaiting clarification of the proposed legislation.

In their short brief to the Task Force, the Telephone Association of Canada says that it has long been concerned with the issue of privacy because it is good business practice.

The Telephone Association acknowledges the potential for invasions of privacy but warns against over-reacting. While they believe that "privacy" should be defined and protected in law, they recommend that security measures be provided on a discriminating basis so that the degree of security and its cost relate closely to some specific need. They believe that the ultimate safeguard of privacy would be to make it a criminal offence to record certain information in any form whatsoever.

CHAPTER 14

COMPUTER SERVICE BUREAUS

Many computer users neither own nor operate their own machines; they find economics dictates that they should instead purchase computing services from a central bureau. In many instances, the individual responsible for files of confidential records at a branch plant or within some department of a corporation is in a like position of customer with respect to his organization's central computing facility. The centralization of computing facilities is becoming an increasingly common phenomenon in government also. The undeniable economy achievable through centralization of computer power is offset in some cases by doubts on the part of the client regarding the degree of confidentiality which will be accorded his data while it is in the hands of the central service bureau. Some of this feeling was evidenced when the National Parole Board told us they remove the "destination" field from the records of notorious convicts before the batchs containing them are delivered to the government's Computer Service Bureau for processing.

We are going to look at three different kinds of computing centres in some detail then examine some security and privacy considerations common to all centres, including owned and operated

ones. The centres to be examined in detail include a centre supplying all computing services to one provincial government; a private centre selling raw computer power on a teleprocessing basis to public and private users (computer utility), and a computer manufacturer which extends computing services to its customers as a collateral function.

The principal privacy issue with regard to computing service bureaus is that files that were formerly kept within the user organizations are now kept, temporarily or permanently, by the service centre. The centres we visited were reluctant to discuss the contents of the files they held for customers. Indeed, some centre officials professed ignorance of the very nature of these files.

Our team that visited the manufacturer's computer centre asked about the nature of customer files held there. No information was volunteered but the company confirmed that some customer payrolls were handled. A good deal of government work passes through the centre; some of this work involves Optical Character Reading and conversion to magnetic tape. The preparation of T-4 Supplementary tapes for National Revenue/Taxation is a case in point. Another job of OCR preparation is done for a provincial personal property security registration system. These tapes and documents are kept up to three weeks by the service bureau.

The computer utility took a like stance, professing ignorance of the nature of customer files handled. They conceded, however, that they process claims files for a provincial health service insurance plan on behalf of a contracting private insurance carrier. This arrangement is being phased out as the province assumes responsibility for processing health service insurance data.

Provincial Computing Centre

The centre does keypunching, key tape preparation, OCR (optical character reading), systems analysis, and programming as well as EDP (electronic data processing). Input consists of documents for keypunching, keying to magnetic tape, or OCR turn-around documents (returned to customer). The centre provides a delivery van service; a sign out/in system is used; mislaid information rarely causes problems and never has information been mislaid without subsequent complete recovery.

Files handled include bank reconciliation for government, bond interest payments, all government payrolls including public servants, teachers, and university staff; sales tax; grading of secondary school final examinations; student aid; health statistics; drivers licences; auto registration; forest inventory; welfare payments (child welfare, long and short term assistance, school allowances); medicare; power commission, payroll and accounts; university computing (registration, grades, transcripts, instruction, and research); government receivables, payables and inventories.

The existing computing equipment configuration will soon be replaced by a large fourth-generation computer.

Student jobs from the university are batch processed but accumulated in a disc area over the reader side of a remote-terminal loop. Limited printout (10 pages maximum) is delivered over the printer side. Connection is by a 2400-baud direct (non-switched) line.

The centre's general policy regarding release of data is that the owner of a file may have access to it by submitting a work order. In general, an individual record can be accessed without a dump of the entire file. Exceptional requests for release of data must be initiated by a letter to the chief executive of the centre. In general, files are not linked although the medical care plan identifying number does appear on motor vehicle registrations. The chief executive of the centre states that any proposed general cross linking of government files would require the assent of the ministers responsible for the files and that, in certain cases, he would seek an opinion in writing from the provincial Minister of Justice. This procedure has been followed in a case where access to the medical care plan file was requested for acquiring population statistics.

Three generations of tape are kept; disc files are dumped on tape for storage. One tape is kept in an off-site vault; most files are on a weekly update cycle -- some are updated daily or monthly. Punched cards are stored in vaults for three years before destruction by incineration; bulk excess printout is incinerated; smaller quantities are shredded.

A great deal of future microfilm activity is predicted should third party microfilming become accepted as legally admissible. It is the understanding of centre officials that federal and provincial courts will accept their own microfilmed documents when presented as evidence. Centre officials have been informed by the provincial Department of Justice that: "Municipal records are acceptable evidence when microfilmed by a third party; and microfilmed records of any crown corporation are acceptable even if the service were performed by their own employees."

There are plans for alternative processing as an emergency back up measure in a comparable computer facility in Montreal.

There are plans to have teletype links to the university and remote video inquiry terminals in government offices. Present plans are that remote job entry from the university would be to the large fourth generation batch-processing computer, whereas terminal jobs would probably be fed to a dedicated time-sharing machine. Communications linkage to the government terminals would be by a 4800-baud direct coaxial line with two multiplexers.

The present policies on release of data and on linking and collating information on file is viewed as placing an unfair burden on centre officials. It would seem that public policy on government information should be established and perhaps a provincial information auditor-general appointed to ensure compliance. As it now stands, public officials of different ministries could cross check files manually by exchanging computer printouts with the onus for any unpopular outcome possibly falling upon the centre. In a sense, the preservation of the individual privacy of the citizens of this province depends upon the philosophy, courage and diligence of one man, the chief executive of the centre, with no force of law nor even of articulated policy to back him up. The requirement for policy articulation notwithstanding, however, there remains among the inherent advantages of centralization the opportunity for implementing proper security and control procedures in one central location.

COMPUTER UTILITY

This company sells computer time; 1/3 of its business is with the federal government, 1/5 with U.S. customers; 120 applications programming systems are offered. This computer utility does not prepare customers' data nor do custom applications programming. No proprietory programmes are offered for sale. The firm employs under 200 staff; half professional-technical, half administrative-clerical. Programming is done for the utility's own system only.

The supervisory control console is on the second floor. On the first floor are control positions for output (paper handling) and tape/disc input. Core dumps go to systems programming offices adjacent to the machine room to diagnose monitor crashes (about two such crashes occur each day).

Customer files are kept on-line (disc) or in removable media -- on private disc packs or tape. There are three levels of storage for removable media; the general file library consists of 11,000 reels belonging to 160 users; a locked restricted library contains 100 - 200 reels. There is also a fireproof storage vault.

There are two kinds of remote service: medium-speed remote job entry and low-speed time-sharing service. The remote-job-entry service has 48 entry ports, some dedicated, serving some 80 terminals of which 20 are in the U.S. Line speeds of 2000, 2400, 3600 and 4800 baud are employed. The low-speed terminals make up a text-preparation system by which jobs are submitted for background batch processing.

SECURITY

Physical. Badge control is in effect. The doors have 10-key combination locks with a 4-digit code. A minimum of four to five operators are on duty at any time. There is no plan for random shift rotation. Operator interventions, for example, the

mounting of tapes, are recorded on the console log. The senior operator controls entry to the computer room; systems programmers and maintenance technicians must do their work under escort. An entry log is maintained. Operators do not program the computer. There is no customer security oversight. A locked room with a remote printer is maintained for "eyes only" paper. The output control operator keeps a trouble-shooting log and shift report on an audio tape recorder. Ionization detectors guard against fire or overheating.

Organizational: There is a Data Security Officer and an Alternate; both reporting to the manager of systems. The Data Security Officer issues passwords and supervises systems security programming. There is no regular review of logs for security purposes. Personnel are cleared by the federal Department of Supply and Services.

Files: Job control cards are analyzed for tape or disc pack requests. A computer-based index programme checks tape serial number against owners' account number and types its output on consoles in the tape library; sometimes there is only one librarian on duty. If the owner's and requester's account numbers don't match, a manual card file is consulted for the owner's written authorization for the requester to use the file or other user-defined security checks. Security has not been requested for on-line files. A library file extraction log is maintained. Each and every access to every file is logged; logs are kept for one week.

On-line files consist of programmes and transaction files. The file password protection scheme provided by the equipment manufacturer has not been automated; the operator must supply the password from a list. It is possible to have privacy transformations on passwords. A user can read another user's files if they are not password protected; however, even the utility's own programmes are not password protected. All writing on files is done with the operator's permission at the user's option. There are no processing authority codes as such; the operator must permit writing on a file; the operator will take action in response to a console command when such a restriction is built into a file. When a flag occurs, the operator checks job numbers and file names.

Teleprocessing: On medium-speed circuits there is a problem in identifying shared ports on both dial-up and direct lines. Sign-on is by password. These passwords are changed by administrative procedure. Reinitialization is necessary after a monitor crash.

There are no terminal identification checks on low-speed circuits. The low-speed sign-in procedure requires the user to transmit his account number (up to eight bytes), user identification (five bytes), and password (up to eight bytes). Access is restricted to files labelled with the user's identification. Write protection is built into low-speed files. A log is maintained of terminal access (sign on/off).

Encryption: Data coming in from remotely entered jobs is scrambled by a simple bit transformation for temporary storage. It is unscrambled for computation, then scrambled again for temporary storage, and unscrambled for delivery to ensure that data goes out with the proper job. Wiretapping on telecommunications lines is not viewed as a serious threat.

MANUFACTURER'S SERVICE BUREAU

The centre maintains a remote operating programming system which is available to all of Canada; and another monitoring system, which is used for applications development. Other services provided include batch-processing operations in which the customer acts as the operator, batch-processing operations using staff operators, input utilizing standard software packages supplied by the manufacturer, and customer input using a custom-made software package, likewise supplied by the manufacturer. The last two services account for the bulk of the data processing activity.

Customers are responsible for arranging with a common carrier for telecommunications resources. The customer must designate the level of security he desires and is responsible for obtaining it from the common carrier. In the principal remote operating system, electronic security consists of a sign-in routine, user identification, password, and project control procedures. Customer data are kept on

discs which are labelled. The operators refer to a table of authorized users when mounting discs and maintain an audit record for control. Separate rooms are provided for customers who come to the centre to process their own data.

A new physical location has recently been established for this computer centre. Security is being provided in the new facility by the design of the physical structure, limitation of access, and software procedures. The firm has a tradition of carefully screening its personnel. In Canada about 20,000 people apply annually for employment; 8,000 are interviewed, and only 1,200 employed. An applicant, in signing the employment application form, consents to the employer obtaining external verification of educational and work experiences, agrees to sign an employee confidential information and invention agreement if employed, and agrees to undergo security clearance if required in the position for which he is ultimately selected. External verification of educational and work experience is generally obtained in writing although the telephone may be used in verifying work experience; if so, the "call back" system is employed. An employee's computerized profile contains, among other data codes, citizenship and indications of the receipt of reports and materials. Each employee is issued an identification card which carries his photograph. A copy of the employee's profile is retained even after he leaves the company's employ.

The company has a blanket bonding policy. Checking of an employee is left to the discretion of his manager; the services of an investigative credit reporting agency may be used. If employees work in government security areas, the government performs security checks on them.

The manufacturer has a separate computing centre to process his own information. The company's manufacturing and laboratory groups each have their own computers.

No terminals are attached to the above mentioned machines as they are dedicated to batch processing. We find this significant. The processing of accounting, personnel, and payroll files occupies one fourth of the machine time. The remaining time is consumed in performing sales and inventory control functions for divisions of the company.

The company centre holds three generations of tape files; the back-up tapes are stored in secure areas. The company is confident that it has adequate physical, hardware, and software provisions for safeguarding the security of the centre and its electronic data processing files.

SECURITY SURVEY

The security provisions implemented by the computer service organizations described, unfortunately, are exceptions rather than the rule.

The security of Canadian corporate, institutional, and some government information systems in general is minimal.

Basically, a corporate information system may involve either batch-processing operation with local job entry only or may have a remote-access time-sharing system. The security risks are greater in the latter case.

In either case the major threats are physical attack: catastrophic destruction, sabotage, theft; and electronic subversion (e.g., embezzlement).

Teleprocessing systems have hazards peculiar to them. Specific threats include unauthorized penetration of the system from remote terminals, and attacks on telecommunications lines, i.e., wiretapping.

Regarding physical attack, an executive of a life insurance company told us:

> "In the U.S. there's been an avowed group that said they're going to get insurance company centres ... They've all had bomb scares ... And people are moving their computers into fortresses. Because let's face it we can't run the business without the computer ... good, bad or indifferent, it's a fact. We can't issue a policy; we can't pay a client,

> can't find anything, we can't do anything. What kind of security system are we moving towards? Fortress, we were doing this in Toronto. We had a thing that was relatively bomb-proof. You know, what's relative? It would take eight sticks of dynamite, which is a fair charge. We haven't got it here but at sometime I think we'll be moving underground, I don't think there's any question."

By the way of contrast, the president of a major fire and casualty insurance company said:

> "Bombs. I was at the home office in Liverpool during the war. One night the Jerries hit us with two big ones. One hit right behind my desk. Glass and plaster all over the place. And the files. Scattered all through the rubble. We had to send a man out on scaffolding to retrieve some of the papers. But by 9:30 a.m. we had it all sorted out. The files were back in cabinets and it was all business as usual. Sure a bomb would be a nasty interruption of our operations but we would survive it."

A major manufacturer, however, is not so optimistic: we were told it has already moved underground -- into an abandoned limestone mine -- to store the great-grandfather back-up tapes of corporate records. And deep within that mine, in a brightly lighted

subterranean amphitheatre there is a large-scale third-generation computer that could, in an emergency, handle the essential data-processing procedures of one manufacturing division.

Catastrophic destruction is not only fear. A large oil company told us it retains specialists on its security staff who try from time to time to penetrate the computer facility and take something or leave something to attest to their visit. If they succeed in a surreptitious infiltration attempt, the operations supervisor on duty would probably be reprimanded for negligence.

This company also has one of the better arrangements for protecting itself from compromise of confidential information during teleprocessing operations. The company has three remote terminals which are linked to its main centre by telecommunications lines. One terminal is used for local job entry; the others for remote job entry. The terminals can access only that data which they have fed into the central computer. The terminals cannot go on line until they have been dialed by the main computer centre; thus all terminal activities are initiated by the centre. Audit logs are also maintained of all teleprocessing activity.

Several computer centres have been victims of physical attack. At Sir George Williams University and at San Francisco State College it was fire; at the University of Wisconsin, a bomb. Other bombing attacks upon computer centres failed to achieve their objectives.

The computing system is a costly and irreplaceable corporate asset. Even if a corporation could raise the capital to replace its computer and get prompt delivery of another, it is highly unlikely any computer user could ever get a direct replacement for its present machine or for its software packages. Engineering changes and variances during manufacturing, and, more importantly, progressive modification of the software practically guarantee it.

Thus far, assaults on computing centres have been frontal ones, noisy and highly destructive. But computers are also vulnerable to more sophisticated forms of sabotage. Small but powerful magnets affixed close to a moving tape or disc surface can wipe or distort information. Diatomaceous earth or corrosive vapours introduced into the air conditioning can initiate pernicious electronic failures. Failures of power supply or air conditioning units or rupture of utility service lines can interdict a computing centre as seriously as its adverse occupation.

Most computer centres we visited had provided for physical protection in depth for processing capability and files. The usual pattern was: three generations of tape files, one on the tape library shelves, one in an on-site fireproof vault, the last in a similar facility off-site; microfilm copies of basic intake documents and COM (computer-output-to-microfilm) copies of changes; and a co-operative arrangement with a "sister" computer in another division or non-competitive outside firm where processing could be done in emergency.

One example of electronic subversion was the infamous sand game which plagued an automobile manufacturer at one time. This gambit necessitated collusion on the part of several employees who set up a fictitious company supplying equally fictitious foundry sand to the corporation. An accounts payable clerk entered the invoices for payment; a receiving clerk entered the deliveries of the non-existent sand; and an inventory clerk entered receipts, requisitions, withdrawals, and even back-orders of the same ephemeral commodity -- and it was a systems analyst who showed them how to co-ordinate their activities in a credible manner. They weren't caught until a company-wide study showed their particular division was using twice as much foundry sand as any other division. Perhaps a 10% overage would have escaped notice, however.

It doesn't always take two or more heads to bilk a corporation. There was the computer programmer who modified his company's payroll programme to accumulate the mil round-off from all withholding tax computations and add it to his own T-4 account; he became suspect when his National Revenue refund cheques began to exceed his basic salary.

The development of teleprocessing has added a new dimension of difficulty to the problem of computer security. A computer cannot tell, in general, which terminal is requesting access, nor can it determine who is using what terminal and consequently what

operations he is privileged to perform or what data he is privileged to see or manipulate. We have found by experimentation that neither can a remote terminal user always be absolutely sure he is in contact with the intended computer.

A salesman for a computer utility faced criminal charges in Alameda City, California for stealing a proprietory programme belonging to a business competitor. He was alleged to have entered his competitor's teleprocessing system using a password obtained from a customer of both computer utilities, and to have had the competitor's programme printed out on a terminal in his own office. The fact that the programme when printed out also produced an unwanted deck of punched cards at the victim's centre was regarded there as an unusual event and led to inquiries regarding this particular entry to the system.

Terminals can be "hard wired" to a teleprocessing system but having a direct line provides no assurance that lines are not interchanged between the terminal and the processor.

In "dial-up" systems, a terminal may be located anywhere. One form of terminal identification widely relied upon is transmitted automatically by an electro-mechanical drum within the calling terminal; a predefined message is transmitted when the computer interrogates the terminal by transmitting a particular ASCII character "here is"; the essential component of this system (the drum configuration) can easily be counterfeited.

A "call-back" system can be provided in which the computer requests terminal identification then breaks off communication and calls back on the listed number of the terminal that purportedly initiated the call; however, this arrangement is little used.

Identification of the user is most frequently relied upon in dial-up systems; conversely in most hard-wired systems, the security of the system depends upon the security of the office in which the terminal is located. Most university records systems using remote access rely upon security of the office housing the terminal. In some hard-wired systems, the office supervisor alone possesses a password needed to open the terminal for the business day; when he closes down the terminal at the end of the day, the computer transmits another password, which the supervisor uses to reopen the terminal; this is one form of a "one-time" password.

In dial-up systems, the user must identify himself by giving his project-programmer pair of numbers and his personal password. Attached to each password is a list of files the possessor is privileged to use and a processing authority code that tells what the possessor is permitted to do with these files. Usually the authority categories are: read only; read and write; or read, write and change the protection of the file. Other systems interrogate the would-be user drawing upon previously stored facts such as his maternal grandmother's maiden name, in this way establishing his identity.

In practice, the simplest security provisions, or none at all, seem to suit systems proprietors the best. Thus for hard-wired systems, reliance is placed on the security of the space housing the terminal; for dial-up systems, the principal means of access control is the password. Only a few systems throw a user off line for giving the wrong password; a would-be infiltrator is thus permitted to try various hunches and permutations of characters which may enable him to gain entry.

Teleprocessing systems are replete with other opportunities for mischief: seizing temporarily detached jobs (even control of the system itself), intruding on another user's communications by way of "talk" circuits, zeroing directories (i.e., wiping out another user's files), "crashing" the monitor at will (thus interdicting all users), dumping residual data left in core memory after having seized additional workspace in core. Keen minds with malicious intent can make a remotely-accessed time-sharing environment a veritable computer jungle. The best protection available at present is afforded by keeping a log of all transactions at all terminals and assiduously investigating all apparent departures from accepted procedures.

There are no known instances of interception of data to attest to the vulnerability of telecommunications lines. However, this may only be because no wiretappers have yet been apprehended

while intercepting data communications. Technically such wire-tapping can be accomplished without serious difficulty. Transmission of digital data over telephone lines is commonly accomplished on low-speed lines by alternately keying two tones of roughly one and two thousand hertz. These signals can be intercepted either by making a metal-to-metal connection across the pair of telephone lines or by placing an inductive coil in close proximity to them. The signals can be recorded on magnetic tape and decoded from a visual display produced by an instrument such as a sound spectrometer. Alternately the signals can be used to actuate appropriate electromechanical printing equipment.

The 110-baud signals to and from a teletype can be recorded on any portable tape recorder and printed out just by playing back the recording into an acoustic coupler attached to another teletype. Signals transmitted over 2400 and 4800-baud lines may require higher quality recording equipment. Multiplexed transmissions present some difficulties in terms of data interception: i.e., procurement or design of specialized demultiplexing and printing equipment or laborious manual decoding and signal analysis with a sound spectrometer, especially since phase modulation is used in many multiplexing systems. Signals at rates of 9600 baud and higher are harder to record, analyze, and decode but these line speeds are not widely used in Canada.

Direct lines afford advantages to the user in terms of convenience and transmission quality but from the security point of view go through the public switched telephone network with the same degree of vulnerability as telephone wires; they may even be tagged with red sleeves for identification by telephone workers, making target identification easier for a potential wiretapper. N.B.: The government's Anti-Wiretap Bill; which received first reading in Commons in July 1971, does not specifically interdict wiretapping on computers. This legislation has subsequently been withdrawn and presumably portions of the bill will be rewritten.

Computers may be utilized to wiretap on computers. A wiretapper can programme a small computer to "spoof" a terminal user -- deceive him into believing he is communicating with the remote computing centre, induce him to reveal his password and other identity codes, then discourage him from remaining on-line by transmitting spurious announcements of system delays or malfunctions -- afterwards the intruder can utilize the access codes he has acquired to gain entry to the system and the victim's files and copy, destroy or alter these files.

The only effective countermeasure against wiretapping is encipherment of all transmission to and from remote terminals. Fortunately, a central computer can be programmed to function as an effective high-speed cipher machine and relatively inexpensive

minicomputers installed at remote terminals can also be programmed to function as cipher machines. However, we discovered no evidence that encipherment is used as a telecommunications security technique in any Canadian systems except those used by the Department of National Defence. Commercial devices for enciphering and deciphering as well as for scrambling telephone conversations are available and some appear to be quite effective.

The possibility of exploiting the near-field radiation from computers and their associated input/output devices has been thoroughly explored by the government of Canada. The extent of this threat and countermeasures against it have been defined in detail. This information is available to computer users possessing a bona fide need to know. In fact, in some cases in which government information is being processed, it is incumbent upon those responsible for the processing that they take appropriate self-defence measures. The initial point of contact for acquisition of information with respect to the security hazards relating to near-field radiation and counter-defences is the Industrial Security Branch of the Department of Supply and Services.

One danger arising from near-field radiation, however, may still remain even in a computer centre which has been adequately shielded and has had its mains supply electrically filtered. This danger arises from the presence of telephone instruments within the inductive field of the computer or its peripheral devices.

The ringing coil of a telephone instrument is an excellent inductive detector; its efficacy is often enhanced when the ringer is altered or retrofitted by the telephone company to respond to a 30 rather than a 20-hertz input signal. Near field radiation picked up by the ringing coil of a telephone instrument can be transmitted even if the handset of the telephone instrument remains upon the switchhook.

Minor modifications to a telephone instrument can, in addition, enable it to pick up and transmit audible sounds in a room when the handset is on the swtichhook and the insinuation of modern miniature semiconductor diodes into the instrument network can make these modifications invisible to most telephone company line-security checks.

CHAPTER 15

THE PRIVACY SURVEY

A survey questionnaire was mailed by the Privacy and Computers Task Force under the imprint of the Federal Departments of Communications and Justice. It was sent to Canadian-based organizations thought to maintain large files of personalized information. It was addressed by name to their chief executive or to the executive directly responsible for data processing. The mailing list was compiled from the Canadian Information Processing Society's current census of Computers, "Canadian Business" lists of largest Canadian industrial and financial organizations, and the membership lists of associations in fields including education, welfare, insurance, health services, and organized labour.

The questionnaire consisted of 124 questions, three of which dealt with verifying the mailing address. The questionnaire was concerned with procedures, policies, practices, and opinion regarding the processing of files of records containing personally identifiable information.

There were five types of questions:

The first type included 29 questions eliciting factual information regarding the activities of the organization, the size and composition of its files, and the characteristics of its electronic data processing equipment.

The second type of question included 28 dichotomous choices; yes or no, and sought information regarding states of being such as perception of hypothetical threats to record-keeping activities, perception of need for new procedural rules and physical safeguards, release of personal information, provision for different levels of confidentiality within a file, provision for translation of data in a record, use of computer service bureaus, detection of errors during computerization, implementation of security measures, effects of computerization, and division of personal data among manual and computerized files.

The third type included 19 questions on a three-point scale: never, occasionally, or frequently; or surrogates of these terms such as: never, as needed, or regularly; or little, marginal, or considerable. These questions dealt principally with information processing practices.

The fourth type included 27 questions on a four-point scale: none, some, most, or all; or never, sometimes, generally, or always. Many of these questions dealt with characterizing the implementation of policy.

The fifth type included 18 questions on a five-point scale: strongly agree, agree, neutral, disagree, or strongly disagree. These questions dealt with opinion regarding record handling policy and regulations.

A pre-test questionnaire was sent to 45 organizations (30 in English, 15 in French). The pre-test elicited 24 responses. The final questionnaire was sent to 2,471 organizations. There were 1,268 responses, including pre-test replies. The basic frequency tabulation was based on the 1,215 earliest replies received. Later cross tabulations included the 43 replies received later. An additional 20 replies were received too late to tabulate.

Close to 200 organizations wrote to explain why they had not returned the questionnaire. The most common reasons were the lack of sufficient knowledge to reply to the questions asked and lack of time. A check of these organizations that did not reply disclosed that the vast majority were small companies or regional associations. Very few, less than 100, operators of large information systems did not reply. Several one-of-a-kind organizations such as National Revenue-Taxation, Statistics Canada, and the RCMP were the subject of site visits by the Task Force and are reported elsewhere in this document. Organizations which did reply to the questionnaire employed about 1.2 million persons, or one-sixth of the labour force. Thus the questionnaire returns,

with due allowance for potential distortions, represented a comprehensive overview of Canadian data banks - or more specifically of data banks containing identifiable personal data about individuals.

The classification of responses according to organizational objectives is:

Not answered	27
Profit making	622
Non-profit	616
Other	3

The classification of responses according to the legal structure of the respondent organization is:

Not answered	55
Federal agencies	55
Provincial agencies	146
Municipal agencies	73
Federally incorporated	302
Provincially incorporated	502
Foreign incorporated	33
Other	102

The classification of responses according to function of the respondent organization is:

Not answered	36
Banking and lending	61
Insurance	76
Public utilities	38
Publishing and mass media	8
Health and vital statistics	182
Education	76
Taxation	2
Motor-vehicles bureaus	2
General merchandizing	22
Oil companies	22
Investment services	64
Law-enforcement agencies	11
Social welfare	39
Chattel mortgage (PPSRS)	1
Credit reporting agencies	10
Service industries	83
Major industrial employers	127
Regulatory agencies	7
Employment agencies	11
Associations	95
Charitable institutions	54
Private investigators, etc.	43
Other	193

The classification of responses according to size (measured by number of employers) of responding organization is:

Not answered	167
100 employees or less	406
100-500 employees	292
500-1,000 employees	142
1,000 to 5,000 employees	194
More than 5,000 employees	67

The more important functions represented by organizations having various types of legal structure are:

FEDERAL AGENCIES

Social welfare	13
Health and vital statistics	9
Services	7
Other	5

PROVINCIAL AGENCIES

Health and vital statistics	38
Education	17
Public utilities	11
Social welfare	9
Associations	8
Charitable institutions	8
Private investigators, etc.	8
Banking and lending	8

MUNICIPAL AGENCIES

Health and vital statistics	16
Social welfare	8
Education	7
Associations	6
Law-enforcement	5

FEDERALLY INCORPORATED

Major industrial employers	89
Insurance	37
Banking and lending	19
Service industries	19
Associations	18
Oil companies	15
Charitable institutions	13
General merchandizing	11

PROVINCIALLY INCORPORATED

Health and vital statistics	94
Investment services	47
Service industries	44
Education	37
Major industrial employers	33
Banking and lending	33
Private investigators	33
Associations	29
Charitable institutions	22
Public utilities	16
Insurance	14
Credit bureaus	6

FOREIGN INCORPORATED

Insurance	19
Associations	4

This analysis is based upon 1,215 questionnaires completed. Not all questions were answered by all respondents: thus we will quote a percentage of the base 1,215 in analyzing the response to each question. Scale variables will be quoted in the form x.xx/N where N is 3,4 or 5 as the case may be. This analysis is based on a tabulation of population variables supplemented by cross tabulations. These cross tabulations are based upon all 1,268 replies. A complete frequency tabulation is given in an appendix.

CHARACTERISTICS OF THE SAMPLE

The classification of organizations responding in a manner amenable to tabulation (82%) is:

Employment area	31.0
Credit area	25.4
Health services	17.9
Welfare area	9.0
Education	7.3
Insurance	7.3
Enforcement area	2.1
	100.0

The employment area included industrial employers, service industries, employment agencies, and associations, principally labour organizations.

The credit area included investment houses, banks and other lending agencies, collection agencies, etc., utilities, merchants, oil companies, credit bureaus, publishers, mailing-list houses, travel and entertainment cards, chattel mortgage registry, and market research.

The last four categories were insignificant in their membership. The welfare area included social assistance agencies and charitable institutions.

The enforcement area included police, regulatory agencies, motor-vehicle bureaus, and taxation. The last two categories had few members.

The classification as to organizational structure (88%) was:

Provincially incorporated	45.5
Federally incorporated	26.6
Provincial agencies	13.4
Municipal agencies	6.4
Federal agencies	5.2
Foreign incorporated	2.9
	100.0

Respondents (99%) were almost evenly divided between non-profit institutions and profit-seeking organizations.

Respondents employed over one million persons, an average of 980 per organization. The largest number of respondents employed less than 100 persons each although 23% of the respondents had 80% of all employees.

"Customers", defined as including present clients, customers, patients, students, policy holders, and members numbered over 65 million; obviously many Canadians were customers of several organizations (88% response). The average organization had 61,000 customers. The most numerous group (326) had between 2,000 and 25,000 customers each, although 14% of the respondents had 83% of all customers.

Only 40% of the respondents said they had files on "subjects", defined to include prospective customers, persons upon whom credit or criminal records were held, auto registrants, and subjects of research studies. Over 34 million records dealt with persons in the "subject" category. The average organization had 70,000 subjects. The most numerous group (233) had less than 1,000 subjects each, although 7% of the respondents had 51% of all subjects.

With regard to information recipients, only 37% of respondents admitted to having any. There were over 2 million recipients reported; the average firm had 4,900; however, 16% of the respondents served 95% of information recipients.

There begins to emerge the picture of an information elite which uses large files of personalized information as its base of power.

Essentially an overview of our sample is as follows: starting with a base of 1,215, we found some responses incomplete or flawed, leaving us with about 1,000 responsive replies. Roughly half of these respondents utilized electronic data processing equipment. Of these, about 300 had their own computers and 200 employed the facilities of computer service bureaus. Of the respondents having computers, about 1/3 had facilities for remote access from terminals.

The tables below summarize the modal characteristics of responding organizations with respect to number of employees, customers, subjects, and information recipients:

CLASSIFIED AS TO OBJECTIVE

Classification	Employees	Customers	Subjects	Recipients
Profit	100	2,000-25,000	0	0
Non-profit	300	2,000-25,000	0	0

CLASSIFIED AS LEGAL STRUCTURE

Classification	Employees	Customers	Subjects	Recipients
Federal Agencies	100	2,000-25,000	0	0
Provincial Agencies	100	2,000-25,000	0	0
Municipal Agencies	300	2,000-25,000	0	0
Federally Incorporated	100	2,000-25,000	0	0
Provincially Incorporated	100	2,000-25,000	0	0
Foreign Incorporated	100	2,000-25,000	0	0
Other	100	1,000	0	0

CLASSIFIED AS TO FUNCTION

Classification	Employees	Customers	Subjects	Recipients
Not answered	100	250	0	0
Banking and lending	100	2,000-25,000	0	0
Insurance	100	100,000	0	0
Public utilities	2,000	100,000	0	0
Publishing & mass media	100	1,000	0	0
Health & vital statistics	300	2,000-25,000	0	0
Education	300	2,000-25,000	0	500
Taxation	300	2,000-25,000	0	0
Motor-vehicles bureaus	300	0	500,000	25,000
General merchandizing	2,000	2,000-25,000	0	500
Oil companies	300	250	2,000	0
Investment services	100	2,000-25,000	0	0
Law-enforcement	2,000	0	100,000	0
Social welfare	100	2,000-25,000	0	0
Chattel mortgage (PPSRS)	300	2,000-25,000	0	25,000
Credit bureaus	100	2,000-25,000	500,000	25,000
Service industries	100	1,000	0	0
Major industrial employers	2,000	2,000-25,000	0	0
Regulatory agencies	100	2,000-25,000	0	500
Employment agencies	300	250	0	0
Associations	100	2,000-25,000	0	0

("Classified as to Function" con'd).

Classification	Employees	Customers	Subjects	Recipients
Charitable institutions	100	250	0	0
Private investigators, etc.	100	250	0	0
Travel & entertainment cards	300	500,000	0	0
Market research	100	250	0	0
Mailing-list suppliers	100	50,000	0	50,000
Others	100	250	0	0

CHARACTERISTICS OF FILES

With regard to international and interprovincial traffic in information, we looked first at the location of files (96%). We found 66% of the files located within any single province, 26% located within Canada, and 8% located partially or entirely in the U.S.A. (Five organizations had their files entirely in the U.S.A.). Organizations most likely to have some files containing personal data located in the U.S.A. were (percentages are based on number of organizations in category):

Oil companies	24%
Associations (esp. labour unions)	20%
Insurance companies	17%
Health services	15%
Manufacturers	13%
Lending institutions	12%

Classified by legal structure, the proportions of organizations having some files in the U.S. were:

Foreign incorporated	46%
Federally incorporated	11%
Federal agencies	7%
Provincially incorporated	4%
Provincial agencies	3%
Municipal agencies	2%

Classified by size (number of employees), the proportion of organizations having some files in the U.S. were:

1,000 to 5,000 employees	11%
over 5,000	10%
500 - 1,000	10%
100 - 500	7%
less than 100	6%

As to location of customers or subjects (79%), we found 40% were entirely within any single province, 35% entirely within Canada, and 25% partially or entirely in the U.S.A. (10 organizations had their customers entirely in the U.S.A.).

As to information recipients (68%), we found 41% entirely within Canada, 31% entirely within any single province, and 28% partially or entirely in the U.S.A (10 organizations had their information recipients entirely in the U.S.A.).

With regard to international traffic in personal information, the frequency with which organizations furnished information to U.S.A. organizations was 1.56/4 (73%); the frequency with which organizations obtained information from U.S. organizations was 1.82/4 (80%): 61 organizations said they frequently supply information to U.S. organizations; 107 organizations said they frequently obtain information from U.S. organizations.

Respondents furnishing or obtaining information to/from U.S.

	Furnish	Obtain
Never	481	383
Occasionally	381	441
Frequently	61	107

Classified by legal structure, the behaviour of organizations with respect to trafficking in personalized information across the Canada/U.S. border was:

Furnishing Information to U.S.

Class \ Frequency	Never	Occasionally	Frequently
Federal agency	28	9	1
Provincial agency	58	44	9
Municipal agency	34	14	4
Federal Inc.	108	102	17
Prov. Inc.	196	162	20
Foreign Inc.	6	10	4

Obtaining Information From U.S.

Frequency / Class	Never	Occasionally	Frequently
Federal agency	20	17	0
Provincial agency	51	47	6
Municipal agency	29	18	5
Federal Inc.	79	124	40
Prov. Inc.	155	188	34
Foreign Inc.	8	7	13

Classified as to function, the organizations most likely to supply personal data to U.S. were:

(Mailing-list suppliers)	
Credit bureaus	90%
Regulatory agencies	58%
Law-enforcement agencies	55%
(Motor-vehicle bureaus)	
Major industrial employers	50%
Insurance companies	46%
Merchandizing houses	46%
Employment agencies	45%

(The parentheses indicate that the response base was too small to calculate a meaningful proportion).

Classified by size, the organizations most likely to supply personalized information to U.S. suppliers were:

Over 5,000 employees	48%
1,000 - 5,000	45%
500 - 1,000	41%
100 - 500	34%
Less than 100	31%

With regard to having electronic data processing done in the U.S.A. (97%), 87% of respondents said they had not considered it; 13% had.

With regard to locating files in the U.S.A. (95%), 76% said they would not do so; 57 organizations said they already had files in the U.S.A. The remainder said they would do so to save money or if they would be placed at a severe disadvantage by not doing so.

The questionnaire requested specific information from each recipient about one selected file, recognizing that every organization had employee files and may have had several types of customer or subject files. The file specified in the questionnaire depended upon the function of the organization and files were specified to give representative coverage throughout our sample. As to classification of files (94%) 14% were concerned with subjects, 31% with employees, and 55% with customers.

The files reported (95%) contained over 83 million records, an average of 72,000 per organization. The most numerous classification (694) had fewer than 5,000 records; however, 19% of the organizations held 90% of the records. Note that it was our usual practice to request inforamtion on what we perceived to be the largest file held by a particular questionnaire recipient.

With regard to size of record (78%), average record size was 520 bytes. However, the largest response category (601) had record sizes under 300 bytes. This was offset by 90 organizations whose record sizes exceeded 2,000 bytes.

Over a million requests a year were reported (72%), an average of 1,300 replies per organization; 791 respondents said they had fewer than 100 requests a year, while 46 organizations said they answered more than 10,000 requests a year.

The tables below summarize the modal characteristics of files responded upon by classification of respondent organizations:

Classification	Type of File	Number of Records	Number of Bytes (Characters)	Annual Requests
Federal agency	Customer	1-5,000	300	100
Provincial agency	Customer	1-5,000	300	100
Municipal agency	Customer	1-5,000	300	100
Federally incorporated	Employee	1-5,000	300	100
Provincially incorporated	Customer	1-5,000	300	100
Foreign incorporated	Customer	1-5,000	300	100
Other	Customer	1-5,000	300	100

Classification	Type of File	Number of Records	Number of Bytes (Characters)	Annual Number of Requests
No response	Customer	1-5,000	300	100
Banking	Customer	1-5,000	300	100
Insurance	Customer	100,000	300	100
Utilities	Customer	1-5,000	300	100
Publishing	Employee	1-5,000	300	0
Health	Customer	100,000	300	100
Education	Customer	1-5,000	300	100
Taxation	Subject	25,000	300	100
Motor-vehicles	Subject	500,000	700	25,000
Merchants	Employee	1-5,000	300	500
Oil	Employee	1-5,000	300	100
Investment	Customer	1-5,000	300	0
Law-enforcement	Subject	100,000	300	500
Welfare	Customer	1-5,000	300	500
PPSRS	-	-	-	-
Credit bureaus	Subject	500,000	300	25,000
Service	Customer	1-5,000	300	100
Industry	Employee	1-5,000	700	100
Regulatory ag.	Customer	1-5,000	300	100
Employment ag.	Customer	1-5,000	300	100
Associations	Customer	1-5,000	300	100

("Classified as to Function" con't.)

Classification	Type of File	Number of Records	Number of Bytes (Characters)	Annual Number of Requests
Charity	Customer	1-5,000	300	100
Investigators	Subject	1-5,000	300	100
T & E Cards	Employee	-	-	-
Market res.	Employee	1-5,000	300	0
Mailing lists	Customer	100,000	2,000	25,000
Others	Customer	1-5,000	300	100

File Characteristics (Modal) By Type of File

Type of File	Number of Records	Number of Bytes (Characters)	Annual Number of Requests Answered
No Response	1-5,000	300	100
Employee	1-5,000	300	100
Customer	1-5,000	300	100
Subject	1-5,000	300	100
Other	1-5,000	300	25,000

Responses about policies regarding obsolete information are summarized below:

Use of purged records by type of file

Use / File	None	Check New Applications	Central repository	Info Exchanged	Response Base
Employees	93	65	20	46	224
Customers	138	158	23	50	369
Subjects	34	33	12	6	85
					678

Future of purged files by type

Future / Type	Destroyed	Returned	Transfer Inactive	Transfer Archives	Response Base
Employees	191	0	85	51	327
Customers	284	4	157	85	530
Subjects	68	0	28	22	118
					975

Time of purging Records by file type

Duration / Type	Immediate	Up to 18 mo.	18 mo. - 7 yr.	7 yr. or more
Employees	21	36	123	138
Customers	23	50	137	332
Subjects	9	6	40	64

Response regarding language in which files were held (96%) showed 76% in English only, 10% in both official languages, 6% in French only, and 8% in coded representation (beyond normal computer code).

Requests for personalized information answered annually by type of file

Number of Requests	Employees	Customers	Subject
Not answered	10	16	7
None	71	170	27
1-100	221	230	72
100-1,000	58	138	30
1,000-10,000	9	63	21
Over 10,000	1	33	12

The average time a record was held after an individual had severed his connection with the organization was 67 months (77%); 534 respondents said they kept such records seven years or more.

Also with regard to records of individuals who severed their connections with an organization (57%): 39% of the respondents said these records were not used; 38% used them to check in case the individual reapplies; 15% exchanged them with other organizations; and 8% sent them to some central registry.

Over age records (81%) were destroyed said 56% of respondents; 27% kept them in an inactive file; 16% sent them to an archival activity. Only four organizations returned them to the subject. Organizations most likely to refer back to old records containing personal data were:

Law-enforcement agencies	100%
Regulatory agencies	100%
(Personal property security registration systems)	
Public utilities	92%
Health services	89%
Educational institutions	88%
Classified by legal structure:	
Provincial agencies	90%
Foreign incorporated	88%
Federal agencies	78%
Provincially incorporated	77%
Federally incorporated	75%
Municipal agencies	71%

Regarding exchange of information with other organizations (96%): 38% said they did exchange information; 62% said they did not.

Most likely to disclose personal data outside their own organizations:

(Motor vehicles bureaus)	
Regulatory agencies	57%
Educational institutions	55%
Credit bureaus	50%
Health services	47%
Insurance companies	45%
Oil companies	45%
Law-enforcement agencies	45%

Classified by legal structure the proportions are:

Provincial agencies:	46%
Federally incorporated	41%
Foreign incorporated	40%
Provincially incorporated	38%
Municipal agencies	29%
Federal agencies	25%

Release of personalized information by type of file:

	Employees	Customers	Subjects
Release	129	258	70
Did not release	238	287	95

We utilized information developed by analysis of responses to the Task Force questionnaire to construct a matrix illustrating the degree of exchange of personalized information among organizations. The column headings designate groups of organizations characterized for the purposes of this study as being primarily information receipients, information suppliers, employers, law-enforcement agencies, health services, educational institutions, or investigatory agencies of a private nature. The column entries characterize their levels of activity as sources of personalized information.

The amount of information made available by each source was estimated from the numbers of requests for personalized information answered annually by the functional types of organizations making up each group. These data were put on a percentage basis by normalizing them with respect to the total number of requests for personalized information reported by all respondents (about 1.2 million requests).

The row headings designate functional types of organizations making up each group of information sources. The row entries characterize their levels of activity as seekers of personalized information.

The level of activity of each seeker was established by weighting the replies to questions dealing with use of sources of personalized information (a weight of 3 for an answer "always used", 2 for "generally used", 1 for "sometimes used", 0 for "never used"). Weighted replies were normalized along each column and the resulting percentages were used to distribute number of requests answered annually by each source group among the functional types of organizations designated by the row headings.

Organizations characterized principally

as information recipients

Credit Grantors	Recipients	Suppliers	Employers	Enforcement	Health	Education	Investigators	Totals
Banking	1.59	.48	.83	.08	.29	.44	.10	3.81
Insurance	1.16	.56	.79	.13	2.02	.42	.27	5.35
Utilities	.98	.32	.57	.11	1.72	.68	.08	4.46
Merchandizing	1.85	.40	1.02	.11	.55	.66	.13	4.72
Oil companies	2.28	.44	.64	.15	1.44	.97	.15	6.07
Investments	1.09	.23	.49	.07	.19	.30	.05	2.42
Subtotal	8.95	2.43	4.34	.65	6.21	3.47	.78	26.83
Welfare								
Welfare	.47	.38	.48	.19	2.08	.87	.20	4.67
Charity	.69	.44	.66	.13	2.72	.84	.07	5.55
Subtotal	1.16	.82	1.14	.32	4.80	1.71	.27	10.22
Group total:	10.11	3.25	5.48	.97	11.01	5.18	1.05	37.05

Organizations characterized principally as information suppliers

	Recipients	Suppliers	Employers	Enforcement	Health	Education	Investigators	Totals
Publishers	.62	.29	.49	0	.42	.95	0	2.77
Motor-vehicles Bureaus	0	0	0	.38	0	0	.14	.52
Chattel Mortgage (PPSRS)	0	0	.68	.38	2.89	0	0	3.95
Credit Bureaus	5.53	.57	1.13	.19	0	.71	.08	8.21
Group Totals:	6.15	.86	2.30	.95	3.31	1.66	.22	15.45

Organizations characterized principally as being in the employment area

Service Indust.	1.38	.37	.77	.16	1.36	.66	.11	4.81
Manufacturers	.73	.27	.93	.20	1.40	.97	.10	4.60
Employment agencies	0	.34	.61	.09	.58	.75	.03	2.40
Associations	.84	.23	.71	.10	.65	.87	.05	3.45
Grand Totals:	2.95	1.21	3.02	.55	3.99	3.25	.29	15.26

Organizations characterized

principally as being in the enforcement area

	Recipients	Suppliers	Employers	Enforcement	Health	Education	Investigators	Totals
Taxation	0	1.02	.68	0	0	0	0	1.70
Law-enforcement	2.42	.47	.60	.82	1.77	1.03	.57	7.68
Regulatory agency	.58	.42	.82	.26	1.93	2.19	.16	6.36
Group Totals	3.00	1.91	2.10	1.08	3.70	3.22	.73	15.74
Health Services	.55	.39	.50	.20	3.18	.48	.12	5.42
Education	.95	.38	.43	.08	1.42	1.83	.03	5.12
Investigators, collection agencies	2.89	.41	.75	.36	.84	.48	.26	5.99
Grand Totals:	26.6	8.41	14.58	4.19	27.42	16.1	2.7	100.00

SECURITY:

Use of different levels of access to files (94%): 35% had it; 65% did not. As to policing the actions of staff with regard to misuse of personal information (93%): 23% of respondents did not police the actions of their own staff; 67% did police the actions of staff but claimed they did not catch any offenders; 10% policed the actions of staff, caught some offenders, and prosecuted or disciplined the ones they caught.

With respect to the likelihood that an organization will take effective action against its own employees for misuse of personalized information in its files (i.e., police, catch, and prosecute):

Non-profit institutions	11%
Profit making organization	7%

Classified by legal structure:

Federal agencies	18%
Provincial agencies	16%
Municipal agencies	12%
Federally incorporated	7%
Foreign incorporated	3%

Most likely to take effective action against their own employees for misuse of personal data:

(Motor-vehicle bureaus)

Law-enforcement agencies	37%
Public utilities	32%
Credit bureaus	20%
Health services	17%

Bilingualism were not an important issue in Canadian records processing generally. There appeared to be a lively exchange of information among organizations.

Organizations tended to leave staff pretty much to their own devices when handling other people's personal information. There seemed to be a tendency to repose a great deal of trust in staff and to close one's mind to the possibility that compromise can occur.

CHARACTERISTICS OF COMPUTER SYSTEMS

The average computer user among our respondents (43%) first began computer processing of records in 1964-65. He went to his present machine in 1967 (33%) - so we were looking at a group of computer users who were broken in on second generation computers and upgraded to third generation machines, in other words, a population of sophisticated users.

First computer use by function

Function \ Date	Before 55	55-60	60-64	64-69	After 69	Response Base
Banking	0	2	7	18	3	30
Insurance	4	6	14	17	12	53
Utilities	1	2	7	15	2	27
Health	0	2	11	48	15	76
Education	1	4	10	32	8	55
Merchandizing	0	2	4	6	1	13
Oil	0	2	6	5	2	15
Investments	0	8	14	13	2	37
Welfare	0	2	1	6	3	12
Service Ind.	2	2	4	13	14	35
Industry	10	13	18	40	7	88
Associations	1	1	1	6	2	11
Other	2	3	13	37	10	65

517

Average memory size (30%) was 133,000 words of core storage - a large machine. In fact, 123 organizations had computers whose memory size exceeded 256,000 words of core storage.

Size of processor by installation date of first computer

Date \ Size	Under 64K	64-256K	Over 256K	Response Base
Before 1964	9	93	49	151
64 - 69	7	92	50	149
After 69	6	33	24	63

363

A 23% response (294) revealed an average on-line disk storage capability of 130 million bytes -- adequate for teleprocessing time-sharing should the user so require.

On-Time Immediate Storage Capacity By Function

Capacity / Function	Under 100 M	100-200 M	Over 200 M	
Banking	8	3	1	12
Insurance	26	8	8	42
Utilities	9	1	4	14
Health	8	6	3	17
Education	15	10	17	42
Merchandizing	8	2	1	11
Oil	9	2	1	12
Investments	2	3	2	7
Welfare	2	1	2	5
Service Ind.	13	4	5	22
Industry	36	18	11	65
Associations	4	1	1	6
Other	26	7	6	39
				294

Only 124 respondents said they had high-speed remote terminals. Of these, 102 had less than six terminals; 22 had six or more. Most users of high-speed remote terminals used them for both input and output (103).

Use of keyboarded remote terminals were reported by 134 respondents; 101 had less than 12 such terminals; 26 had from 12 to 200 terminals; only 7 had more than 200 keyboarded terminals. Most users had input and output capability of these terminals (81), but significant numbers restricted the terminals to either input alone (18) or display only (15).

Security (38%): 73% of respondents had implemented physical access controls over electronic data processing equipment; 39% had implemented hardware or software security measures such as passwords, terminal identification code, or cryptographic coding (this compared well with the proportion of systems capable of time sharing); 42% ran personal integrity checks on data processing personnel; 58% reported utilizing audit logs or other data monitoring methods; 69% employed secure disposal methods for unwanted tapes or printouts; and 31 respondents reported implementing security measures beyond those suggested on the questionnaire.

Manual Files-Supplementary (35%): 90% of respondents said they supplemented their computer based files of personal information with manual files; 83% said these files contained more subjective data than the computer files; 70% said these data were more narrative in nature; and 75% said they were more sensitive from the standpoint of confidentiality.

Experience With Computers: The importance of the computer (39%) has principally been to improve routine processing operations, said 51% respondents; it results in more complete and timely reports (45%); only 4% said it permits better management planning, as its major advantage.

However, respondents (41%) rated the computer at 2.42/3 in terms of value to an organization.

During the process of computerizing files of personal data, 74% of respondents said they detected errors in their existing manual files (33% response), and the importance of correcting these errors was rated 1.76/3 (24% response). The importance of accuracy problems experienced with the computer was rated 1.36/3 (40% response).

Appreciation of computer technology enabled an organization to pull together, in one record, all information it collected and stored on a given individual according to 32% of respondents (38% response). Only 16% said that, as a result of increased retrieval capability after computerization, they were called upon to furnish more individually identifiable information to government agencies; and only 34% said that, as a result of computerization, they were called upon to furnish more statistical (aggregated) information regarding individuals.

The amount of data collected per given individual after computerization was rated 2.36/3 (33% response). However, only 39% of respondents attributed this increase to the fact of computerization; on the other hand, 60% attributed the primary reason for increased data collection to changes in organizational objectives or programmes, or to increasing government requirements for collecting or reporting information (18% response).

Only 4% of respondents said that new rules regarding the individual's privilege to examine his record in a file had been issued since their organization began using computerized record systems. Only 80 respondents replied to a question that attempted to link such rules to the fact of computerization and of these only 11 attributed the new rules to computerization.

Only 19% of respondents (34% response) said they were considering additional uses (such as sale of mailing lists or preparation of market estimates) for personal information then in computer based files.

Utilization of Computers: With regard to the proportion of employees on whom computerized records were maintained, respondents (40%) rated it 2.73/4; with respect to the amount of such information computerized given the total amount held, the rating was 2.07/4.

With regard to the proportion of customers on which compterized records were maintained, respondents (38%) rated it 3.16/4; with respect to the amount of information computerized given the total amount held, the rating was 2.53/4.

With regard to the proportion of subjects on which computerized records were maintained, respondents (21%) rated it 2.0/4; with respect to the amount of information computerized given the total amount held, the rating was 1.84/4.

Extent of Computerization of Employee Records

By File Size

Size \ Extent	None	Some	Most	All	Response Base
Under 100	59	11	4	22	96
100 - 500	49	14	13	52	128
500 - 1000	16	4	8	50	78
1000 - 5000	16	15	34	74	139
Over 5000	2	14	8	30	54

495

Extent of Computerization of Subject Records
By File Size

Size \ Extent	None	Some	Most	All	Response Base
None	63	14	8	8	93
1 - 2000	27	20	3	7	57
2000 - 25,000	12	9	8	13	42
25,000 - 100,000	7	7	4	11	29
100,000 - 500,000	8	3	4	3	18
Over 500,000	6	6	6	5	23

262

Extent of Computerization of Customer Records
By File Size

Size \ Extent	None	Some	Most	All	Response Base
None	13	2	1	2	18
1 - 250	10	8	7	21	46
250 - 2000	10	13	11	39	73
2000 - 25,000	10	24	28	103	165
25,000 - 100,000	7	11	15	32	65
100,000 - 500,000	4	13	19	41	77
Over 500,000	1	8	13	16	38

482

Summary: We see the computer-using half of our survey population as utilizing modern and sophisticated equipment with somewhat greater potential for teleprocessing than has been exploited thus far.

Data security practices were somewhat less formal than one would have imagined. The more technically sophisticated users appeared to share a better appreciation of the value of security than their more pedestrian counterparts.

Almost universally, computer based files were supplemented by manual files and it was in the manual files where we found the information that constituted the greater potential for invasion of individual privacy.

The computer has been used principally as a tool to cope with routine record-keeping function and its potential for decision-making was largely unexploited.

If anything, the computer has contributed to more accurate record-keeping and has not introduced any significant new problems in this regard. Given the fact that 3/4 of all organizations found their manual files to be in error when they began computerizing, one wonders about the remaining manual files, which were said to contain far more sensitive information about individuals.

The ability of the computer to pull together hitherto uncollated facts regarding individuals was just beginning to be exploited as was the ability of organizations to find new uses for personal data now rendered more easily accessible.

The fact of computerization did not appear to generate any new requirements for gathering or disseminating data regarding individuals, but the computer did make it possible for organizations to respond to requirements that arose from the increasing complexities of society itself.

Organizations had given little apparent consideration to the rights of subjects regarding their records and to any role the computer could play in implementing such rights once defined.

Both in number of persons concerned and amount of data describing each, the computer had been applied most vigorously to customer, employee, and subject records, in that order.

INFORMATION GATHERING PROCEDURES

Several questions sought to learn the principal general sources from which organizations gathered information regarding the individuals upon whom they maintained records. Each of the following general sources was rated on a 4-point scale (none, some, most, or all); the percentage response on the base 1215 is quoted in each case.

Individual on whom the record was kept	2.88/4	(86%)
Other information suppliers	1.52/4	(89%)
Investigators	1.26/4	(89%)
Published sources or public records	1.19/4	(89%)
Information recipients	1.14/4	(89%)

(i.e. merchants in the case of credit bureaus)

Organizations most likely to use investigators to gather personal data were:

Law-enforcement agencies	100%
Insurance companies	70%
Private investigators	49%
Social welfare agencies	46%
Regulatory agencies	43%
Credit bureaus	40%
Merchandizing houses	37%
Major industrial employers	31%

Classified by legal structure the proportions were:

Foreign incorporated	58%
Federal agencies	48%
Municipal agencies	37%
Provincial agencies	31%
Federally incorporated	31%
Provincially incorporated	21%

Most likely to obtain personal data regarding the subject from educational institutions:

Employment agencies	92%
Publishers	88%
Regulatory agencies	85%
Educational institutions	81%
Social welfare agencies	77%
Major industrial employers	77%
Oil companies	58%
Credit bureaus	50%

Most likely to seek personal data from the families of subjects:

(Personal Property Security Registration Systems)

Health services	84%
Social welfare agencies	80%
Charitable institutions	80%
Law-enforcement agencies	72%
Insurance companies	65%
Private investigators	65%

Classified by legal structure the proportions were:

Municipal agencies	74%
Provincial agencies	69%
Federal agencies	60%
Foreign incorporated	58%
Provincially incorporated	47%
Federally incorporated	29%

Most likely to obtain personal data regarding the subject from law-enforcement agencies:

(Personal Property Security Registration Systems)	
Law-enforcement agencies	82%
Regulatory agencies	57%
Private investigators	55%
(Motor-vehicles bureaus)	
Insurance companies	43%
Major industrial employers	40%

We next sought information regarding the specific sources which might be interviewed or otherwise approached for information regarding individuals. Again, a 4-point rating scale was used (never used, sometimes, generally, or always); the percentage response on the base 1215 is quoted in each case.

Subject himself	2.85/4	(94%)
Medical practitioners and hospitals	2.26/4	(82%)
Referees nominated by the subject	2.20/4	(83%)
Former employers of the subject	2.03/4	(80%)
Subject's present employer	2.01/4	(75%)
Educational institutions attended by subject	1.90/4	(79%)
Members of the subject's family	1.71/4	(85%)
Law-enforcement agencies	1.44/4	(75%)
Subject's neighbours or friends	1.40/4	(81%)

Organizations most likely to obtain personal data regarding the subject from medical sources were:

(Personal Property Security Registration Systems)	
Health services	89%
Insurance companies	82%
Social welfare agencies	82%
Charitable institutions	74%
Regulatory agencies	72%
Law-enforcement agencies	63%
Major industrial employers	62%

Classified by legal structure the proportions were:

Provincial agencies	70%
Foreign incorporated	67%
Federal agencies	60%
Federally incorporated	50%
Provincially incorporated	48%
Municipal agencies	17%

Most likely to seek personal data from the subject's employer:

(Personal Property Security Registration Systems)	
Merchandizing houses	73%
Employment agencies	73%
Insurance companies	70%
Law-enforcement agencies	63%

Major industrial employers	59%
Banking & lending institutions	58%
Private investigators	58%
Regulatory agencies	57%
Social welfare agencies	57%

Classified by legal structure the proprotions were:

Foreign incorporated	40%
Provincial agencies	36%
Federal agencies	35%
Federally incorporated	33%
Provincially incorporated	25%
Provincial agencies	14%

Most likely to seek personal data from the friends and neighbours of subject:

(Personal Property Security Registration Systems)	
Health services	80%
Educational institutions	79%
Insurance companies	65%
Law-enforcement agencies	63%
Social welfare agencies	52%
(Tax authorities)	
Private investigators	49%

Classified by legal structure the proportions were:

Foreign incorporated	48%
Provincial agencies	38%
Municipal agencies	29%
Provincially incorporated	28%
Federal agencies	25%
Federally incorporated	24%

Finally, we sought information regarding the methods used by representatives in approaching sources to induce them to furnish information regarding individuals. A 4-point rating scale was used (never used, sometimes, generally, or always); the percentage response on the base 1215 is quoted in each case.

Identify the organization represented	3.01/4	(63%)
Identify himself and present credentials	2.78/4	(68%)
Demonstrate that the subject has consented to the gathering of information about him	2.76/4	(56%)
Disclose the reason for the inquiry	2.41/4	(47%)
Promise to protect the informant	2.73/4	(49%)
Guarantee the ultimate use to which information will be put	2.38/4	(49%)
Confirm facts from at least two independent sources	2.25/4	(53%)

The lower percentage response to the last set of questions doubtless arose from the fact that the question implied use of investigation procedures that were not within the context of some information systems.

In response to the questions as to whether the individuals upon whom records were kept or groups representing their interests ever complained against the method of collecting any item of information (88%) the rating was 1.16/3. Only five organizations said they got frequent complaints, 910 said they got none at all.

Most likely to receive complaints regarding methods of collecting personal data:

Law-enforcement agencies (Motor-vehicles bureaus)	55%
Credit bureaus (T & E cards)	50%
Insurance companies	49%
Social welfare agencies	44%
Oil companies	23%
Educational institutions	22%

Classified by legal structure the proportions were:

Foreign incorporated	30%
Municipal agencies	20%
Federal agencies	18%
Provincial agencies	16%
Federally incorporated	14%
Provincially incorporated	12%

Questionnaire responses classified by type of file were:

Complaints Regarding Collection of Personalized Information

Frequency / Type	Never	Occasionally	Frequently
Employees	322	18	1
Customers	461	122	1
Subjects	127	24	2

Not surprising was the fact that the subject himself was the prime source of information. More surprising was the fact that health service was in second place. One would have expected references to be checked, but it was interesting that they turned out to be more important sources than former employers, present employer, or educational institutions. Rather surprising were the facts that public records were rarely consulted and that law enforcement agencies were sources at all.

It was interesting that individuals seeking information did in fact let sources know whom they represented. Other ratings regarding methods might be subject to some modification were distinction made between sensitive personal information and more innocuous information.

INFORMATION DISSEMINATION PROCEDURES

Three questions explored the relative use of different means of disseminating personal information. These were rated on a 3-point scale (never used, occasionally, or frequently). In each case percentage response on the base 1215 is quoted.

Information was furnished in response to specific requests	2.09/3	(86%)
Special reports were distributed selectively	1.56/3	(73%)
General reports were published periodically	1.32/3	(70%)

As to management policies regarding disclosure of personal data (96% response), 55% of respondents said they had an unwritten policy, 33% had a written policy, and the rest had none at all.

With regard to having a written disclosure policy:

Non-profit institutions	44% (had)
Profit making organizations	19%

Classified by size:

500 - 1,000 employees	48%
1,000 - 5,000 employees	41%
100 - 500 employees	39%
more than 5,000	30%
less than 100	19%

Existence of Disclosure Policies by Type of File

	Employees	Customers	Subjects
None	53	56	27
Unwritten	259	321	77
Written	56	269	60

We enquired whether an explicit statement of the organization's policy was communicated and scored responses on a 3-point scale (never, as needed, or regularly). In each case percentage response on the base 1215 is quoted:

Employees charged with records		
Management	2.54/3	(81%)
General Public	2.27/3	(44%)
Individuals whose records were held	1.81/3	(75%)

Response to the question as to whether individuals on whom records were kept or groups representing their interest ever complained about disclosure of personal information (82% response) evoked a score of 1.13/3. Only four organizations said they got frequent complaints; 873 said they got none at all - practically the same response pattern as in the case of complaints about data collection.

Most likely to receive complaints regarding disclosure of personal data:

(Motor-vehicles bureaus)	
Credit bureaus	60%
Educational institutions	28%
Law-enforcement agencies	18%
Social welfare agencies	18%
Employment agencies	18%
Health services	14%
Regulatory agencies	14%

Classified by legal structure the proportions were:

Provincial agencies	16%
Municipal agencies	14%
Federal agencies	11%
Foreign incorporated	10%
Provincially incorporated	10%
Federally incorporated	8%

POLICY IN DEALING WITH SUBJECTS

The right of an individual to examine his own record or a copy of his record from the file was the cornerstone of many suggested reforms in the area of privacy of individual information.

Following is a complete tabulation of answers to the question of whether or not this right existed:

	Number	Per Cent
No response	64	5.27
The individual did not know the record existed	62	5.19
He had no understanding of the contents of his record	135	11.03
He could examine all data in his record	502	41.87
He could examine some data in his record	291	23.21
He could examine no data in his record	172	14.24

Right to Examine One's Personal Record

by Type of File

	Employees	Customers	Subjects
Did not know record exists	9	43	10
Had no understanding of contents	31	85	19
All	169	257	76
Some	133	121	37
None	22	131	19

In cases where an individual was permitted to examine data in his record, we asked whether translation or interpretation was provided to an official language which the individual understood (79% response); 68% said it was.

Organizations least likely to permit an individual to examine all data on his record included:

(T & E cards)	
(Market research firms)	
Insurance companies	5%
Social welfare agencies	9%
Law-enforcement agencies	10%
Health services	20%
Employment agencies	23%
Oil companies	23%

Classified by legal structure the proportion were:

Foreign incorporated	12%
Provincially incorporated	33%
Federal agencies	36%
Federally incorporated	40%
Provincially incorporated	43%
Municipal agencies	47%

Response to the question of whether individuals on whom records were kept or groups representing their interests had ever sought to examine their own records or complained about the adequacy of an organization's practices regarding an individual's right to examine his own record (87% response) evoked a score of 1.20/3. Only eight organizations said they got frequent requests; 867 said they got none at all -- again a response pattern similar to those questions regarding collection and dissemination.

Most likely to receive complaints about the inability of a subject to examine his record:

Law-enforcement agencies	50%
Credit bureaus	40%
Health services	35%
Regulatory agencies	29%
Social welfare agencies	26%
Public utilities	26%
Educational institutions	23%

Classified according to legal structures the proportions were:

Federal agencies	29%
Municipal agencies	25%
Provincial agencies	20%
Provincially incorporated	18%
Federally incorporated	12%
Foreign incorporated	6%

Complaints Concerning Inability to Examine One's Personal Record

Type \ Frequency	Never	Occasionally	Frequently
Employees	293	38	3
Customers	446	128	4
Subjects	128	26	1

ADDITIONAL STUDIES

Twenty-four questions dealt with attitudes of the information system proprietors comprising our sample. These questions concerned attitudes regarding threats to record systems, record-keeping procedures, rights of subjects, and regulation. Except for six dichotomous choices, all these questions were scored on a 5-point scale (strongly agree, agree, neutral, disagree,

strongly disagree). A value of 1 represents strong disagreement. We will be reporting average scores and quoting percentage response on a base of 1215.

THREATS

We asked how the respondent organizations perceived the following events as serious threats to their record-keeping activities.

Carelessness or indiscretion of employees	46% yes (95%)
Theft or unauthorized alteration	38% yes (93%)
Wilful destruction (e.g., bombing)	34% yes (95%)
Unauthorized telephone interception	17% yes (93%)

Particularly striking were the lack of fear of wiretapping and the recognition of employee carelessness or indiscretion as the major threat.

We stated the proposition that information-systems proprietors should furnish data to law-enforcement officers on demand (i.e., without demanding they get a warrant); score was 2.94/5 (95% response). Interestingly, this was the second most unpopular proposition.

However, the over-all response was biased by heavy participation from health services and educational institutions. A functional breakdown disclosed the following types of organization in agreement that data banks should be opened to law-enforcement officers on demand:

Banks
Insurance
Utilities
Merchants
Oil companies
Credit
Service industries
Industrial employers
Regulatory agencies
Employment agencies
Associations

Classified by legal structure the groups in agreement with this principal included:

Federal agencies
Federally incorporated
Provincially incorporated
Foreign incorporated

Then we stated that files should periodically be purged of obsolete information: score was 1.48/5 (95%). No disagreement of any kind was detected.

RIGHTS OF SUBJECTS

We stated the premise that records were the exclusive property of information system proprietors and that subjects had no residual interest in them -- score 3.14/5 (95%). It was encouraging to see that information system proprietors had this appreciation of the rights of subjects; this was the most unpopular proposition among our attitudinal questions. However, general merchandizing houses and credit bureaus were in agreement.

Next we advanced six propositions articulating claimed or proposed rights of subjects on whom records containing personally identifiable information were maintained.

To be informed of the existence of such records when they were started 1.82/5 (94%)

Credit bureaus voiced strong disagreement.

To correct, rebut, update, and expunge incorrect or obsolete information concerning them 1.88/5 (94%)

No groups recorded disagreement.

To review on demand the contents of records concerning them 2.25/5 (95%)

Insurance companies and health services reported disagreement; law-enforcement agencies and regulatory agencies recorded strong disagreement.

To learn the sources of information concerning them 2.52/5 (74%)

Insurance companies and health services reported disagreement; law-enforcement agencies and credit bureaus recorded strong disagreement. Foreign incorporated organizations reported disagreement.

To be furnished periodically with an accounting of its uses made of information concerning them 2.73/5 (94%)

The following types of organizations disagreed:

Insurance

Health

Merchandizing

Oil companies

Police

Credit *

Industrial employers

(* means "strong disagreement").

Classified as to legal structure, groups reporting disagreement included:

Provincial agencies

Municipal agencies

Federally incorporated

Provincially incorporated

Foreign incorporated

To stop the exchange of information concerning them among information suppliers 2.75/5 (94%)

All groups, classified by legal structure, reported disagreement. The following groups, classified by function, reported disagreement:

Banks

Insurance *

Utilities

Health

Merchandizing

Oil companies

Investments

Police

Credit *

Services

Industry

It was encouraging and a little surprising to observe the absence of strong disagreement among information system proprietors regarding these claimed or proposed rights of subjects.

ATTITUDES REGARDING REGULATION

Twenty-three per cent of respondents (97% response) agreed that new and more detailed organizational rules were needed to govern collection and use of personal data; 77% said their present rules or practices were adequate. No variation from this pattern was noted by cross tabulation.

Four questions concerned the desirability of actions regarding data banks containing personally identifiable data:

Establishing standards concerned with the acquisition and dissemination of information 1.73/5 (92%)

(No variation from this pattern was noted by cross tabulation).

Establishing standards of hardware and software security 1.82/5 (91%)

(No variation from this pattern was noted by cross tabulation).

Registration as to purpose and contents 1.85/5 (93%)

Publishers reported strong disagreement; oil companies reported disagreement.

Periodic site inspections 2.10/5 (91%)

Publishers and credit bureaus reported strong disagreement. The low incidence of disagreement was striking.

Five questions concerned the desirability of licencing and certification of different categories of individuals concerned with the operation of information systems dealing with personally identifiable information:

Information suppliers 1.54/5 (93%)

(Publishers only disagreed, strongly).

Data-bank proprietors 1.58/5 (93%)

(Publishers only disagreed, strongly).

Data processing centres 1.84/5 (93%)

(Publishers disagreed strongly; merchandizing houses and oil companies disagreed).

Data gatherers 1.92/5 (93%)

(Publishers disagreed strongly; merchandizing houses and oil companies disagreed).

Computer programmers 2.18/5 (93%)

The class of federally incorporated firms disagreed with this suggestion. Disagreement was reported by the following functional classifications:

Banking

Publishers *

Merchandizing *

Oil companies

Major industry

We took note once again of a low incidence of strong opposition to regulation. It was interesting that agreement was strongest with respect to licencing of management personnel rather than professionals, as one might have expected.

It may have been, however, that private organizations in the business of third-party exchange of personalized information looked towards licencing as a legitimation of their activities, conferring some sort of quasi-official status such as enjoyed by private investigators.

Over-all one gathered the impression that the information processing industry was cognizant of the potentiality of modern information processing technology to lessen the quality of life by invasion of individual privacy and would welcome guidelines within which they could utilize this new technology without creating social problems and with the assurance that their more vociferous competitors would not overstep these bounds to the detriment of society at large and to the commercial disadvantage of other information systems proprietors.

Notes on Use of Rating Scales

In some of the tables above, the general source (e.g.) "Individual on whom the record was kept" was scored 2.88/4.

This result can be visualized as a point on a line:

1	2	3	4
	X		
None	Some	Most	All

which is the average value of all (1144) responses to this particular question.

In some of the tables above, the means of dissemination "Information was furnished in response to specific requests" was scored 2.09/3. This result can be visualized as a point on a line:

1	2	3
	X	
Never used	occasionally used	frequently used

which is the average value of all responses to this particular question.

In some of the tables above, the proposition "Subjects had the right to be informed of the existence of such records when they are started" was scored 1.82/5. This result can be visualized as a point on a line:

1	2	3	4	5
X				
Strongly agree	Agree	Neutral	Disagree	Strongly disagree

which is the average value of all responses to this question.

APPENDIX 1

METHODOLOGY FOR DATA GATHERING

Empirical studies for the Task Force were carried out by a team consisting of two computer scientists, a sociologist, and a management consultant assisted by five graduate students. To this team were seconded from time to time public officials from the Departments of Justice and Communications. The officials were by professional training lawyers, computer scientists, or sociologists. Also seconded to the empirical studies team were other consultants to the Task Force, principally academics -- lawyers or computer scientists for the most part.

Our studies entailed a) solicitation of briefs from 187 Canadian industrial and professional associations; b) conduct of 43 site interviews; c) the preparation, testing and mailing of a questionnaire to 2516 data-bank proprietors; d) and undertaking field studies in Toronto, Montreal, and London consisting of media search and introspective studies to characterize the effects of invasion of privacy upon individuals.

BRIEFS

Briefs were solicitated from all interested parties thought to be sufficiently well organized to participate in filing. The substance of the briefs covered, in general, the submittor's

concept of privacy and the means by which this concept is implemented. Sixteen associations notified us of their intent to file briefs. Briefs were received from the:

Retail Council of Canada

Retail Credit Company of Canada Ltd.

The Royal Bank of Canada

The Canadian Life Insurance Association

The Telephone Association of Canada

Canadian Association of Data Processing Service Organizations (brief to CCCTF)

The Canadian Medical Association

Committee of Presidents of Universities of Ontario

The Canadian Banker's Association

United Community Fund of Greater Toronto

Ontario Medical Association

Canadian Book Publisher's Council

Canadian Copyright Institute (joint brief)

sufficiently early in our work to influence subsequent directions.

Site interviews took place in Vancouver, Winnipeg, London, Toronto, Oshawa, Ottawa, Montreal, Quebec City, and St. John's. They were set up well in advance of our visits and officers to be interviewed were furnished an advance copy of the questions to be asked.

We used three or four man interview team, Anglophone or Francophone as required. Its composition changed depending upon the site visited. There was usually a computer scientist and a lawyer; the remaining members could include sociologists or a management consultant. During interviews, we used a tape recorder set up in clear view on a desk or table. It was used only with the interviewee's permission and turned off when so requested. Interviewees who asked to hear the tape after the interview were sent duplicated cassettes. Generally, the tape was viewed as a back-up to interview notes. In some cases tapes were transcribed word-for-word; in others, graduate students listened to the tape and paraphrased important passages as an alternative to complete transcription.

Prior to each site interview we held a background briefing of the team. At this briefing, we distributed a profile of the organization to be visited. Source materials used in making up the profile included annual reports, advertising materials, speeches by officials, information from standard reference sources, stories clipped from back issues of national, local, employee, and union newspapers pertaining to major events, changes in records handling procedures, systems changes, new equipment configuration, confrontations, consumer or worker complaints, or intramural dissonance which might be relevant to the problem of information handling.

A control form was prepared for each visit detailing the interview schedule, times, dates, and those present. The teams used a standard interview aid listing general areas of interest and affording space for copious note taking. Interviews took up to 2½ hours depending principally upon the responsiveness and level of preparation of the subject.

Our broad areas of interest included: a) the data processing organization, b) an inventory of files containing personally identifiable information, c) a summary of the characteristics of each file, e) utilization or potential utilization of teleprocessing, f) known violations of confidentiality, confrontations, or perceived threats to security, g) and plans for future expansion or systems modification.

We considered it essential that the file inventory be complete regardless of whether the files were computerized or not. These files typically included: personnel files, customer or subject files, and special files -- e.g., warrantee, equipment.

The heart of the study lay in summarizing the characteristics of each file. The contents could often be gleaned from a record image. In addition we sought to find out what documents provided input data, how much was carried over, where, how long, and under what conditions of confidentiality and security the input documents (and intermediate document images such as punched cards) were stored -- and how they were eventually disposed of; also whether they were microfilmed.

We attempted to determine whether the contents contained items of information that could be used to contravene any applicable Human Rights Code.

We asked how data was acquired: whether from the subject, third parties, hearsay, or copied from other records.

We probed into what backup records were provided (how many generations and update cycle) and what their security was (vault storage, off-site storage, full-time tape librarian, etc.).

We studied the distribution of hard copy printout (or location and accessibility of terminals) and the means for wiping tapes, zeroing core, and destroying carbons, ribbons, and spoiled printouts; what administrative use was made of copies distributed and what accountability was required for copies of multipart forms. We looked for evidence of photocopying, Multilith reproduction or removal of records from the custodial area.

We sought to find out which officers had accountable responsibility for each record, to whom and under what conditions data might be released, and whether log books and a receipt system were maintained; we asked for specific incidents in which information had been supplied to other organizations, police forces, government agencies, foreign embassies, credit bureaus, parents and spouses, or individuals. We asked about incidents (e.g. disciplinary action taken against employees) that would tend to show whether action were being taken to assure compliance with existing regulations.

We attempted to determine how long and in what form records were retained, and especially what became of the records of ex-customers, unsuccessful applicants, and former employees, and what use, if any, was made of them.

We asked if formal or informal agreements existed for interchange of records with other agencies or institutions.

We investigated procedures used to verify the accuracy of intake records such as key punch verification or use of confirmation copies -- and whether such copies were accounted for or could become the basis for personal ad hoc files.

If teleprocessing was used for files containing personally identifiable information or if such use seemed imminent, our procedure was to enquire regarding the security (from wiretapping) of interconnecting transmission lines, ascertain the physical security of the remote terminals and the means by which each terminal identified itself to the computer, the electronic means of access to the system or how each terminal user identified himself to the computer, processing restrictions placed on files, whether a log was maintained of each terminal session (including unsuccessful attempts to gain access) and who had the responsibility of analyzing entries on the audit log for possible compromise.

Additional documentation was usually requested during the interview. These documents included: intake forms, record images (usually card or tape formats), output documents, titles of computer programmes, and descriptions of computer configurations.

Statements of policy were likewise collected such as copies of resolutions, guidelines or codes of ethics, employee handbooks, compilations of rules and regulations, statements of policy, declarations of confidentiality, and release forms for personal information.

Each team leader had the responsibility for analyzing information adduced during a site visit. He usually had been present at all interviews (although not necessarily as the principal interviewer). He read all profile materials, examined all documents, and interview transcripts, and reviewed the results of any collateral studies (see below).

He sometimes drew a rough organizational chart showing the place of the records-keeping and data-processing activities within the organization under study and a flow chart of each records system showing the movement of intake forms, confirmation copies, and output documents between offices and files.

He usually looked at each identifiable type of record to see if he could chart how and from what sources the information was acquired, what forms it assumed, what output documents were generated and what ultimately became of each input form, copy, and output document.

If any step seemed unclear, the team leader framed a clarifying question to be submitted to the officer concerned.

The leader then wrote a 250-word summary of the main points of the visit in terms of privacy and security of personal information. This summary was sent to all members of the site interview team for comments and further questions. These questions and other questions which might have occurred to the team leader were sent, together with a revised summary, to the officer who was responsible for co-ordinating the visit. This officer then obtained answers to the questions posed and checked the summary for factual accuracy.

The team leader then compiled a final critical report on the organization.

MAIL QUESTIONNAIRE

We compiled a 124-question mail questionnaire. This was sent to named individuals at 2471 companies, agencies, and insitutions throughout Canada. The list was compiled from the following sources: the Canadian Information Processing Society Census of Computers (about 1700 relevant entries); lists compiled by Task Force members in Toronto, Montreal, Winnipeg, and London; the largest Canadian corporations (industrial and financial -- Canadian Business), membership lists of associations of organizations in fields such as finance, health care, insurance, law-enforcement, and social service, and federal and provincial government directories.

Prior to sending out the main questionnaire, a pre-test was conducted over a list of 45 organizations selected on a stratified sampling basis. This pre-test, which produced a response in excess of 50%, resulted in significant restructuring of the survey questionnaire.

FIELD STUDIES

Collateral studies were conducted in London, Toronto and Montreal. Local publicity that our study was under way triggered some private communications from individuals which revealed sensitive areas to probe during site interviews.

We also asked members of the study team to compile profiles of the items of information they thought might be stored on them in records; then we checked these suppositions with facts developed during the site visits.

Where the media search conducted during the background investigation revealed any particularly relevant cases of invasion of privacy, it was sometimes useful to contact the reporter and compile details of the case. Issues developed were sometimes raised during site interviews to obtain the views of responsible officials.

Our field studies consisted also of a media search of newspapers and magazines of general interest and of those serving the data processing field. We were also able to establish informal working relationships with Opportunities for Youth and other groups operating in fields involving legal aid, consumer protection, and studies of community service functions. Through these contacts we obtained case history material which proved useful in several contexts during our investigations.

AMERICAN STUDIES

In an attempt to secure data upon which to evalute the extent to which Canadian citizens have become entries in U.S. personal information systems, we mailed letters of inquiry to 19 American organizations which we had reason to believe had in their files personalized data regarding Canadians. We inquired as to what data were stored, what they were used for, and what rights were accorded the individuals concerned or described.

We requested information from the following U.S. organizations: American Airlines Inc.; American Express; Beneficial Finance; Carte Blanche; Diners Club Inc.; Hilton Hotel Corp.; Household Finance Corp.; ITT Data Processing; Institute of Electrical and Electronics Engineers; McGraw-Hill Data Services; Merill, Lynch, Pierce, Fenner and Smith; National Data Corp.; Recording and Statistical Corp.; Retail Credit Corp.; Sheraton Corp. of America; TRW Credit Data Corp.; Wellington Fund Inc.; Credit Index; and Casualty Index.

We received replies from: American Airlines Inc.; American Express; Carte Blanche; Diners Club Inc.; ITT Data Processing; Institute of Electrical and Electronics Engineers; McGraw-Hill Data Services; National Data Corp.; Recording and Statistical Corp.; Retail Credit Corp.; TRW Credit Data Corp.; Credit Index; and Casualty Index. These replies were regarded as briefs and information extracted from them is reported at appropriate places in the body of this report. With the exception of a flag used to signify that billings should be in Canadian funds, the records were generally the same as those of their U.S. counterparts or records of a similar type (travel-and-entertainment cards, professional membership) kept by Canadian organizations in comparable activities. The Recording and Statistical Corp. (MIB) segregated Canadian records as a group.

In the cases where application was made for credit, the application came under the U.S. federal Fair Credit Reporting Act. In the event the application was refused on the basis of a report filed by a credit reporting agency, the applicant must be informed of the fact and furnished the name of the agency turning in an unfavourable report. He then had the right to visit an office of that agency and see the file concerning him upon which the unfavourable report was based. If he did not agree with the report, the credit reporting agency was obligated to reinvestigate his case and file another report. If the subject believed that additional information was required to have his case understood in a proper light, he might file a brief (up to 100 words long) to the point with the credit reporting agency and the agency was required to make it part of his file, and send out copies of it to everyone who had received a report on that individual in the last six months.

Presumably a Canadian visiting a bureau in Canada would be accorded the same rights as an American visiting one in the U.S. if his inquiry was triggered by notification from a U.S. based credit grantor, especially since nearly all Canadian credit reporting agencies were branches or affiliates of U.S. firms. Canadians seeking credit from Canadian credit grantors had no such enunciated rights.

On the other hand, records concerning or describing Canadians held in U.S. based information systems were subject to seizure by American authorities in the same way records concerning Americans would have been.

APPENDIX 11

STRUCTURE OF THE PROBLEM

The structural framework upon which this report was built was erected upon the Social Contract model, that is, the claimed right to privacy notwithstanding the individual may be obliged to surrender some personal information concerning or describing himself if he seeks some benefit from society; and that society has the need to gather certain personal information concerning or describing individuals to ensure its proper functioning and to guarantee the rights of others.

We characterized systems in terms of what benefits they were capable of granting or what functions of society the proper functioning of which they were established to ensure. Upon examining the characteristics of the organizations studied during site visits we perceived seven benefits: employment, medical care, consumer credit, education, social assistance, insurance, and the privilege of owning or operating a motor vehicle. Similarly, we perceived three social functions: taxation, administration of criminal justice, and social planning (census). This left the computer service bureaus as odd men out, but for convenience we could regard them as employers in the context of this particular model.

As a next step, we made a subjective grouping of the organizations visited under the 10 denominations outlined above. It was, of course, recognized that several organizations could have fit into two or more categories. However, this fact would have done nothing to invalidate this approach and accordingly we made our judgments based upon our motives in visiting each of the sites, i.e., the kind of personal data file we were most interested in studying.

The resulting groupings are as follows:

Employment:

MacMillan Bloedel Ltd.

General Motors of Canada Ltd.

Public Service Commission.

IBM Canada Ltd.

Systems Dimensions Ltd.

Newfoundland and Labrador Computing Services Ltd.

Industrial Security Branch, Dept. of Supply & Services.*

Hickling-Johnston (employment agency).

Credit:

Bank of Montreal (chartered bank)

Caisse Populaire Desjardins (near bank)

Avco Financial Services (finance company)

Nesbitt-Thompson (investment house)

Credit: (Con'd.)

The Royal Bank - Chargex (bank card)

Air Canada (travel-and-entertainment cards)

CN Hotels (travel-and-entertainment cards)

Shell Canada Ltd. (oil company credit cards)

Supertest Petroleum Ltd. (oil company credit cards)

Robert L. Simpson Ltd. (department store)

Dupuis Freres (department store)

Ontario Hydro (public utility)

Bell Canada (public utility)

British Columbia Telephone (public utility)

Credit Bureau of London (credit reporting - filed based) *

Retail Credit Canada Ltd., Toronto (credit reporting - investigatory)

Retail Credit Canada Ltd., Winnipeg(" " ")

Dun and Bradstreet of Canada Ltd. (credit reporting - mercantile)

Hooper-Holmes Bureau Inc. * (credit reporting - investigatory)

Personnel Property Security Registration System (credit reporting - registry)

Canadian Consumer Loan Association *

File Underwriters Investigating Bureau *

Medical Care:

Clarke Institute of Psychiatry

Hôpital Notre Dame

Ontario Health Services Insurance Plan

Social Assistance:

National Health and Welfare

Vancouver Department of Social Services

Service du Bien - Etre Social (Montreal)

Education:

North York Board of Education

Université du Québec

Insurance:

London Life Insurance Co.

Royal Group Insurance Companies*

Motor Vehicles:

Motor Vehicles Branch, Manitoba Department of Transport

Taxation:

Department of National Revenue/Taxation

H. & R. Block Canada Ltd.

Justice:

Solicitor-General's Department

R.C.M.P.

Canadian Penitentiary Service

National Parole Board

Toronto Metropolitan Police

London Police Department *

Census:

Statistics Canada (DBS)

* Informal visit, interview, or profile study only.

We constructed a 10 x 10 matrix of which the 10 categories or systems comprised the row and column headings. In each cell intersection we placed a number denoting the level of activity of the corresponding row heading (agency i) as an information seeker with respect to the corresponding column heading (agency j) as a source.

We recognized five levels of information transfer activity perceived during site interviews appreciating the fact that in a given interagency relationship several levels of information transfer might exist simultaneously. Weight values were assigned to each level of activity which were selected according to two criteria: weight values would connote increasing degrees of invasion of personal privacy; and any permissible logical combination of activity states would yield a unique sum of weight values.

The scheme for quantifying information transfer activity is detailed as follows:

Level 1: Agency i obtained aggregated statistical data regarding the involvement of individuals with agency j. Weight value 1.

Level 2: Agency i occasionally collected data from individuals regarding their involvement with agency j. Weight value 2.

Level 3: Agency i regularly collected data from individuals regarding their involvement with agency j. Weight value 4.

Level 4: Agency i regularly went to agency j to obtain data regarding an individual's involvement with it. Weight value 12.

The resulting matrix is:

Seekers	Credit	Taxation	Insurance	Justice	Welfare	Employment	Motor Vehicles	Census	Medical	Education	Totals
Credit	17	10	16	10	10	16	16	1	11	10	117
Taxation	8	17	16	6	16	17	8	1	10	10	109
Insurance	16	2	17	9	8	10	17	1	17	10	107
Justice	10	8	9	17	10	10	17	1	11	10	103
Welfare	10	17	10	8	17	17	10	11	10	10	120
Employment	8	4	3	10	4	17	8	1	11	17	83
Motor Vehicles	6	6	11	17	6	4	17	1	11	3	82
Census	2	17	3	17	5	5	5	17	4	5	80
Medical	2	8	10	8	10	5	4	1	17	4	69
Education	4	8	2	2	10	11	4	1	4	17	63
Totals	83	97	97	104	96	112	106	36	106	96	931

The most active seekers after personal information may be seen to be:

Welfare	120
Credit	117
Taxation	109
Insurance	107
Justice	103

The most productive sources of personal information may be seen to be:

Employment	112
Medical	106
Motor Vehicles	106
Justice	104

Correlations obtained were as follows:

	Credit	Taxation	Insurance	Justice	Welfare	Employment	Motor Vehicles	Census	Medical	Education
Credit	1.0000									
Taxation	-.2594	1.0000								
Insurance	.6869	-.0283	1.0000							
Justice	-.0468	-.0229	-.0574	1.0000						
Welfare	.1857	.5785	.4340	-.4962	1.0000					
Employment	.5301	.2138	.1989	-.4976	.5015	1.0000				
Motor Vehicles	.7522	-.3911	.6044	.4718	-.0675	.0289	1.0000			
Census	-.3158	.6751	-.3640	.3138	-.0018	-.1517	-.3338	1.0000		
Medical	.3981	-.5099	.6354	-.0170	-.0502	-.0537	.3970	-.5034	1.0000	
Education	.2370	-.2195	-.3229	-.5747	-.0510	.6870	-.1717	-.2853	-.2751	1.0000

We saw the important correlates with each system were:

Credit:	Motor vehicles, insurance, employment
Taxation:	Census, welfare
Insurance:	Credit, medical, motor vehicles
Welfare:	Taxation, employment
Employment:	Education, credit, welfare
Motor Vehicles	Credit, insurance
Census:	Taxation
Medical:	Insurance
Education:	Employment

A principal axis factor analysis was performed on these data. Nine eigenvalues were found to be significant with a 0.0 cutoff. The resulting factor matrix was as follows:

	FACTOR								
	I	II	III	IV	V	VI	VII	VIII	IX
Credit	.8455	-.1533	.1425	.4281	.1434	.1711	.0059	.0322	-.0853
Taxation	-.5167	-.3847	.7461	.0668	-.0534	-.0651	-.1216	.0387	-.0216
Insurance	.7980	.0216	.5230	-.1743	-.0177	.1400	-.1800	.0401	.0700
Justice	-.1108	.8080	.2362	.4435	-.0544	-.2748	-.0140	.0616	-.0013
Welfare	.1771	-.6586	.6009	-.2621	-.1893	-.0811	.2497	.0137	-.0088
Employment	.3367	-.8267	.0365	.3251	.1324	-.2365	-.1294	-.0762	.0119
Motor Vehicles	.7501	.3961	.1734	.4318	-.2031	.0147	.1336	-.0572	.0362
Census	-.6936	.0514	.4848	.3172	.3790	.1316	.332	-.0150	.0418
Medical	.7289	.2812	.0283	-.4623	.3596	-.1978	.0799	.0194	-.0004
Education	.0969	-.7058	-.6110	.3181	.0135	-.0204	.0785	.0946	.0486

If we look at only positive factor loadings and take a loading of 0.1 or more as signifying a major component, we perceive seven significant factors.

Factor I includes as major components: credit, insurance, motor vehicles, medical and to a lesser extent, employment and welfare, and as a minor component, education. We may conveniently interpret this as the "eligibility for insurance" factor.

Factor II includes as major components justice, motor vehicles and medical, and as minor components, census and credit. We may conveniently interpret this as the "right to drive" factor.

Factor III includes as major components taxation, welfare, insurance, census, justice, motor vehicles, and credit, and as minor components, employment and medical. We may conveniently interpret this as the "benefit means test" factor.

Factor IV includes as major components justice, motor vehicles, credit, employment, education, and census, and as a minor component, taxation. We can call this the "employment selection" factor.

Factor V, the last one about which meaningful conclusions can be drawn, includes census, medical, credit, and employment as major components and education as a minor component. This could be called the "social planning" factor.

Factor VI with credit, insurance, and census as major components and motor vehicles as a minor component seems closely related to Factor I while Factor VII with welfare, motor vehicles, and credit as major components and medical and education as minor components seems closely related to Factor III.

Appendix III

PRIVACY AND COMPUTERS TASK FORCE

THE DEPARTMENT OF COMMUNICATIONS/THE DEPARTMENT OF JUSTICE

SURVEY QUESTIONNAIRE

Definitions

An Individual's Record is a set of one or more consecutive units of information on a single individual (e.g., an employee's history of employment, a payroll record).

A File is a collection of related records treated as a unit, e.g., a file on all employees of the organization.

Manual Files are records (including microfilm) which are maintained and accessed by hand.

Electric Accounting Machine (EAM) Files are records which are typically accessed and manipulated by using electro-mechanical devices such as card sorters, tabulating machines, collators, etc.

Computerized Files are records which are maintained in card, tape, disc, drum, or core storage, and are manipulated by a computer.

Section 1

Questions 1 to 6 concern your organization and its record-keeping activities generally without reference to any particular file or to the use of computers

1. A. Respondent identification number. [ ]

1. B. Who will complete this questionnaire? (Mark one response only).
The person to whom the questionnaire was sent ( )
Someone else (please specify) ( )
[ ]

1. C. Where are the officers principally responsible for records processing located? (Mark one response only).
The address to which this questionnaire was sent ( )
Some other address (please specify) ( )
[ ]

2. A. How is your organization characterized with respect to legal structure? (Please mark one response only). Ø = 55

Federal Agency	(55)
Provincial Agency	(142)
Municipal or regional agency	(68)
Federally incorporated	(283)
Provincially incorporated	(484)
Foreign incorporated	(30)
Other (please specify)	(98)

2. B. How is your organization characterized with respect to objectives? (Please mark only one response). Ø = 26

Profit-making	(588)
Non-profit	(596)

2. C. How do you characterize the prime function of your organization? (Please mark only one category). Ø = 36

Banking, lending and other financial institution	(57)
Life, accident, or casualty insurance	(73)
Public utilities	(37)
Publishing and mass communication media	(7)
Health or vital statistics	(179)
Education	(73)
Taxation	(1)
Driver licencing or auto registration	(2)
General merchandizing	(19)
Travel and entertainment cards or reservations	(1)
Oil company	(18)
Investment service	(62)
Law enforcement, probation, parole	(11)
Social welfare or benefits	(38)
Chattel mortgage registration	(1)
Credit information exchange	(7)
Service industry	(79)
Major industrial employer	(128)
Regulatory agency	(7)
Employment agency	(11)
Market research	(1)
Association (labour, professional)	(92)
Charitable organization	(51)
Mailing-list supplier	(2)
Private investigator, collection agency, insurance adjuster, etc.	(42)
Other (please specify)	(188)

3. Do you maintain any records on individuals in the following categories? (Please mark one response in each category).

3. A. Number of Employees (present full-time employees at all levels in your organization).

Ø = 159

100	(398)	1,000-5,000	(185)
100-500	(289)	Over 5,000	(56)
500-1,000	(136)		

3. B. Number of Clients or Customers (e.g., present clients, customers, patients, students, policy holders, members, etc.).

Ø = 48

None	(97)	25,000-100,000	(107)
1-250	(247)	100,000-500,000	(98)
250-2,000	(243)	Over 500,000	(49)
2,000-25,000	(326)		

3. C. Number of Subjects (e.g. prospective customers, persons upon whom credit and criminal records are held; auto registrants and licencees; research subjects; etc.).

Ø = 124

None	(599)	25,000-100,000	(63)
1-2,000	(233)	100,000-500,000	(37)
2,000-25,000	(124)	Over 500,000	(35)

3. D. Number of Information Recipients (e.g., merchants, credit grantors, prospective employers, etc.).

Ø = 121

None	(644)	1,000-50,000	(63)
1-500	(349)	Over 50,000	(10)
500-1,000	(28)		

4. Does your organization perceive the following hypothetical events as serious threats to your record-keeping activities? (Please mark one response in each row).

		Ø	Yes	No
4. A.	Willful destruction (e.g. bombing)	72	(391)	(750)
4. B.	Theft or unauthorized alteration	83	(427)	(703)
4. C.	Unauthorized telephone interception	89	(188)	(937)
4. D.	Carelessness or indiscretion of employees	66	(528)	(621)

5. A. This question concerns the physical location of records, subjects or client/customers, and information recipients. (Please mark one response in each row).

	Entirely within a single province	Entirely within Canada	Partially in the USA	Entirely in the USA	Does not apply	
5.A.1 (Ø=27)	(771)	(299)	(86)	(5)	(27)	Records
5.A.2 (Ø=91)	(387)	(334)	(227)	(10)	(166)	Subjects or client/customers
5.A.3 (Ø=122)	(198)	(266)	(172)	(10)	(453)	Information recipients

5. B. Please mark the statement which best defines your working relationship with U.S. based suppliers of information (e.g. credit bureaus, etc.) (Please mark one response in each row).

	Never	Occasionally	Frequently	Do not know	Does not apply	
5.B.1 (Ø=45)	(457)	(368)	(59)	(8)	(277)	We furnish information
5.B.2 (Ø=68)	(364)	(421)	(184)	(7)	(249)	We obtain information

5. C. Have you ever seriously considered having portions of your data-processing operations performed in the U.S.?

Ø = 39 Yes 151 No 1022

5. D. Under what conditions would you locate files in the U.S. (Please mark one response only). Ø = 56

Files are now in U.S.	(57)
If it made sense economically	(112)
Only if put to a severe disadvantage by not doing so	(109)
Under no foreseeable circumstances	(880)

6. A. Given your understanding of the balance between organizational needs to collect information and the individual's interest in the confidentiality of his record, please indicate which of the statements (a or b) in each set best applies. (Please mark only one response in each pair).

6. A.1 a) We need new and more detailed organizational rules to govern collection and use of personal data. (242) Ø = 39

b) Our present rules or practices are adequate (931)

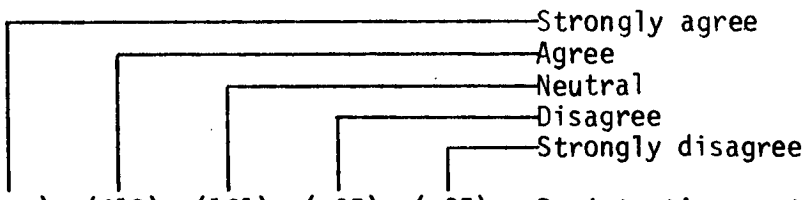
6. A.2 a) We need additional physical safeguards on collection storage, and distribution of personally identifiable information. (229) Ø = 43

b) Our physical safeguards are now adequate. (942)

6. B. Subjects on whom records containing personally identifiable information are maintained should have the following rights. (Please mark one response in each row.)

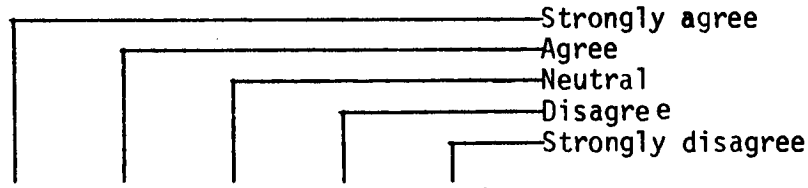
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	
6. B.1 Ø = 78	(450)	(431)	(147)	(82)	(27)	To be informed of the existence of such records when started.
6. B.2 Ø = 66	(330)	(421)	(121)	(186)	(91)	To review on demand the contents of records concerning them.
6. B.3 Ø = 78	(422)	(478)	(97)	(88)	(52)	To correct, rebut, update, and expunge incorrect or obsolete information concerning them.
6. B.4 Ø = 77	(202)	(243)	(257)	(327)	(109)	To be furnished periodically with an accounting of the uses made of information concerning them.
6. B.5 Ø = 76	(232)	(357)	(193)	(244)	(113)	To learn the sources of information concerning them.
6. B.6 Ø = 82	(232)	(211)	(207)	(344)	(139)	To stop the exchange of information concerning them among information suppliers.

6. C. The following actions regarding data banks containing personally identifiable data are necessary. (Please mark one response in each row).



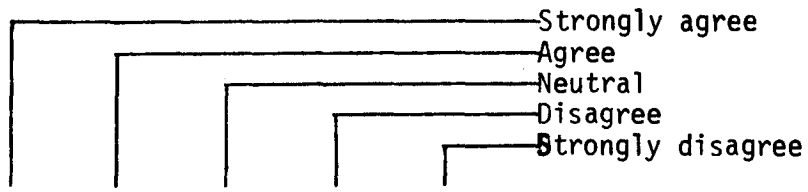
6. C.1 Ø = 93	(422)	(419)	(161)	(95)	(25)	Registration as to purpose and contents.
6. C.2 Ø = 120	(368)	(440)	(206)	(58)	(23)	Standards of hardware and software security.
6. C.3 Ø = 103	(435)	(461)	(143)	(49)	(24)	Standards concerned with the acquisition and dissemination of information.
6. C.4 Ø = 108	(291)	(391)	(275)	(99)	(51)	Periodic site inspections.

6. D. The following people and organizations trafficking in personally identifiable information should be licensed and certified. (Please mark one response in each row).



6. D.1 Ø = 86	(592)	(362)	(112)	(44)	(19)	Data-bank proprietors
6. D.2 Ø = 90	(606)	(356)	(114)	(33)	(16)	Information brokers (suppliers)
6. D.3 Ø = 89	(479)	(346)	(188)	(86)	(35)	Data-processing centres
6. D.4 Ø = 91	(376)	(255)	(265)	(176)	(52)	Computer programmers
6. D.5 Ø = 88	(446)	(336)	(205)	(101)	(39)	Data gatherers

6. E. Please mark one response in each row.



6. E.1 Ø = 68	(93)	(189)	(107)	(433)	(325)	Records are the exclusive property of the information-system proprietors subjects have no interest in them.
6. E.2 Ø = 72	(123)	(351)	(158)	(286)	(225)	Information-system proprietors should furnish personal data to law-enforcement officers on demand.
6. E.3 Ø = 67	(395)	(585)	(82)	(60)	(26)	Files should periodically be purged of obsolete information.

SECTION 2

Questions 7-14 refer to the file of records specified in the cover letter. In answering these questions please furnish information with respect to this file alone.

7. Classification of file. Please mark the one response that best describes the file about which you are furnishing information.

Ø = 64

Your own employees	(352)
Clients or customers	(633)
Subjects	(165)

8. A. Please indicate the approximate number of individuals on whom records are maintained in this file. (Please mark only one response).

Ø = 62

1-5,000	(694)	50,000-500,000	(178)
5,000-50,000	(228)	Over 500,000	(53)

8. B. Please indicate the approximate size in characters (bytes) of an individual record in this file. (Please mark only one response).

Ø = 253

1-300	(601)	700-2,000	(109)
300-700	(162)	Over 2,000	(90)

8. C. Please indicate the language in which these records are stored. (Please mark only one response). Ø = 51

English	(882)	Both official languages	(118)
French	(77)	Coded	(87)

9. Do you ever make individually identified information from this file available to persons or organizations outside your own (except as required under federal or provincial law):

Ø = 48	Yes	(449)	No	(718)

10. A. How is individually identified information from this file disseminated to information recipients? (Please mark one response in each row).

	Never	Occasionally	Frequently	Do not know	Does not apply	
10. A.1 Ø = 84	(660)	(106)	(82)	(4)	(279)	General reports are published periodically.
10. A.2 Ø = 90	(502)	(267)	(112)	(9)	(235)	Special reports are distributed selectively.
10. A.3 Ø = 56	(172)	(600)	(268)	(7)	(112)	Information is furnished in response to specific requests.

10. B. Please indicate the approximate average number of specific requests fulfilled annually. (Please mark only one response). Ø = 66

None	(270)	1,000-10,000	(98)
1-100	(524)	Over 10,000	(44)
100-1,000	(221)		

11. A. Is there a general management policy regarding disclosure of personally identified information? (Please mark only one response). Ø = 48

No policy has been formulated	(138)
Yes, we have an unwritten policy	(646)
Yes, we have a written policy	(383)

11. B. Is an explicit statement of the policy communicated to the following groups? (Please mark one response in each row).

	Almost never communicated	Discussed as the need arises	Regularly communicated	Does not apply	
11. B.1 Ø = 66	(247)	(594)	(72)	(235)	Individuals whose records are maintained in this file.
11. B.2 Ø = 66	(46)	(377)	(566)	(159)	Employees charged with records management.
11. B.3 Ø = 73	(243)	(215)	(35)	(647)	General public.

11. C. Do you ever take disciplinary action against your own employees for violation of confidentiality? (Please mark only one response).

Ø = 69

We do not police the actions of our employees	(269)
We police the actions of our employees and haven't discovered any violations of confidentiality.	(763)
We police the actions of our employees and have prosecuted violations of confidentiality when discovered.	(114)

11. D. Are different provisions concerning disclosure attached to different portions in this file?

Ø = 67 Yes (361) No (787)

11. E. Have individuals on whom records are kept or groups representing their interests ever complained about disclosure of information in this file to people outside your organization? (Please mark one response in each row). Ø = 47

Never	(873)
Occasionally	(121)
Frequently	(4)
Do not know	(135)
Does not apply	(35)

12. A. As a general rule, can the individual examine his own record or a copy of his record from the file? (Please mark only one response).

Ø = 64

The individual does not know the record exists	(63)
Has no understanding of the contents of his record	(134)
Can examine all data in his record	(499)
Can examine some data in his record	(282)
Can examine no data in his record	(173)

12. B. If an individual is permitted to examine any data in his record, is translation or interpretation provided to an official language which the individual understands?

Ø = 260 Yes (649) No (304)

12. C. Have individuals or groups representing their interests ever sought to examine their own records or complained about the adequacy of your organization's practices regarding an individual's right to examine his own record? (Please mark one response only).

Ø = 56

Never	(862)
Occasionally	(190)
Frequently	(8)
Do not know	(61)
Does not apply	(38)

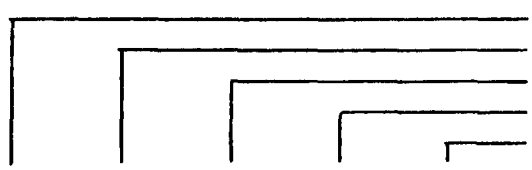
13. A. Indicate your principal means for gathering information for this file? (Please mark one response in each row).

	None	Some	Most	All	
13. A.1 Ø = 133	(451)	(530)	(67)	(34)	Other information suppliers
13. A.2 Ø = 144	(744)	(288)	(26)	(13)	Published sources or public records.
13. A.3 Ø = 78	(63)	(211)	(474)	(396)	Individual on whom the record is kept.
13. A.4 Ø = 139	(819)	(212)	(33)	(12)	Information recipients (e.g. merchants
13. A.5 Ø = 130	(745)	(264)	(48)	(28)	Investigators

13. B. Have individuals on whom records are kept or groups representing their interests ever complained against the method of collecting of any item of information in this file? (Please mark one response only). Ø = 46

Never	(903)
Occasionally	(159)
Frequently	(5)
Do not know	(69)
Does not apply	(32)

13. C. Please indicate whether any of the following sources are used in collecting identified information about individuals for storage in your files? (Please mark one response in each row).



13. C.1 Ø = 48	(30)	(109)	(288)	(711)	(37)	Subject himself
13. C.2 Ø = 71	(454)	(448)	(98)	(27)	(116)	Members of subject's family
13. C.3 Ø = 77	(641)	(318)	(22)	(9)	(149)	Subject's neighbours or friends
13. C.4 Ø = 73	(220)	(482)	(203)	(102)	(135)	References nominated by subject
13. C.5 Ø = 77	(304)	(413)	(176)	(78)	(167)	Former employers of subject
13. C.6 Ø = 80	(298)	(396)	(126)	(89)	(226)	Present employer
13. C.7 Ø = 67	(352)	(310)	(167)	(168)	(151)	Medical practitioners and hospitals
13. C.8 Ø = 72	(574)	(299)	(25)	(18)	(226)	Law enforcement agencies
13. C.9 Ø = 72	(378)	(386)	(119)	(81)	(186)	Educational institutions attended by subject.

13. D. Please indicate which of the following techniques are used by your representatives in collecting identified information about individuals for storage in your files? (Please mark one response in each row).

	Never used	Sometimes used	Generally used	Always used	Does not apply	
13. D.1 Ø = 79	(93)	(95)	(211)	(420)	(317)	Identify himself and present credentials.
13. D.2 Ø = 94	(122)	(110)	(167)	(360)	(362)	Identify his employer
13. D.3 Ø = 94	(116)	(107)	(154)	(372)	(372)	Disclose reason for investigation
13. D.4 Ø = 96	(162)	(87)	(96)	(250)	(524)	Promise to protect informant.
13. D.5 Ø = 104	(177)	(68)	(95)	(255)	(516)	Guarantee the ultimate use of information
13. D.6 Ø = 99	(140)	(142)	(147)	(252)	(434)	Demonstrate that the subject has consented to the gathering of information about him.
13. D.7 Ø = 100	(161)	(244)	(149)	(85)	(476)	Confirm facts from at least two independent sources.

14. A. When an individual on whom records are kept is denied the benefit he seeks or severs his relationship with your organization, how long is his record retained? (Please mark one response only). Ø = 55

Record is immediately purged	(55)
Retained up to 18 months	(94)
Retained from 18 months to 7 years	(301)
Retained 7 years or longer	(540)
Do not know	(60)
Does not apply	(110)

14. B. When records are purged from this file, what is done with them? (Please mark one response only). Ø = 50

They are destroyed	(549)
Returned to the individual on whom they are kept	(4)
Transferred to an inactive file	(271)
Transferred to an archival activity	(161)
Do not know	(26)
Does not apply	(154)

14. C. What use is made of the retained record of an individual who is denied the benefit he seeks or severs his relationship with your organization (include inactive and archival records). (Please mark one response only). Ø = 67

These records are not consulted	(269)
They are used to check new applications to our organization	(258)
Data from them are sent to a central repository	(55)
Information is exchanged with other organizations	(105)
Do not know	(45)
Does not apply	(416)

SECTION 3

THE FOLLOWING QUESTIONS (15-22) REFER TO YOUR ORGANIZATION'S USE OF COMPUTERS OR COMPUTING SERVICES WITHOUT REFERENCE TO ANY PARTICULAR FILE, IF YOU DO NOT USE COMPUTERS, PLEASE STOP HERE AND RETURN THE QUESTIONNAIRE TO US AT YOUR EARLIEST CONVENIENCE.

THANK YOU FOR YOUR CO-OPERATION

15. A. When did you first use a computer system to store and process records? (Please mark only one response). Ø = 691

Before 1955	(23)	1964-1969	(265)
1955-1960	(51)	After 1969	(81)
1960-1964	(102)		

15. B. When was your present central processor installed? (Answer in respect of your principal computer used in processing records). (Please mark only one response). Ø = 689

Prior to 1964	(34)	After 1969	(130)
Between 1964 & 1969	(240)	Does not apply	(122)

15. C. What is the core capacity of your central processor in computer words? (Please mark only one response). Ø = 714

Less than 64,000	(156)	Greater than 256,000	(65)
Between 64,000 and 256,000	(145)	Does not apply	(135)

15. D. What is the on-line immediate-memory storage capacity of your computer in characters (bytes)? (Please mark only one response).

Ø = 723

Less than 100 million	(164)	Greater than 200 million	(56)
Between 100 and 200 million	(65)	Does not apply	(207)

16. A. Do you maintain computerized records on any (none, some, most, or all) of your employees, clients/customers, and subjects? (Please mark one response in each row).

	None	Some	Most	All	Does not apply	
16. A.1	(145)	(57)	(62)	(218)	(32)	Employees
Ø = 701						
16. A.2	(50)	(79)	(88)	(249)	(49)	Clients/Customers
Ø = 700						
16. A.3	(122)	(59)	(31)	(45)	(235)	Subjects
Ø = 723						

16. B. Given the total information on each employee, client/customer, or subject, how much of the information is in computerized form? (Please mark one response in each row).

	No information	Some information	Most information	All information	Does not apply	
16. B.1	(125)	(203)	(121)	(20)	(50)	Employees
Ø = 696						
16. B.2	(39)	(236)	(141)	(43)	(58)	Clients/Customers
Ø = 698						
16. B.3	(103)	(85)	(38)	(14)	(251)	Subjects
Ø = 724						

17. A. What has been the principal effect on your organization of computerizing your records? (Please mark only one response).

Ø = 691

Improvement in routine, large-scale operations	(241)
Generation of more timely or complete reports	(213)
Direct improvement in policy planning	(18)
No basis for comparison	(51)

17. B. Which of the following statements best describes your experience with computer data-processing applications? (Please mark only one response).

Ø = 689

We could not manage files of such size and complexity as ours without a computer	(228)
The applications have provided a useful improvement in operations but we could continue service without a computer	(251)
The applications have had relatively little impact on our use of files	(20)
No basis for comparison	(26)

18. Who generally operates the computer system for handling records containing individually identified information. (Please mark only one response).

Ø = 694

We have our own in-house computer system	(314)
We use a service bureau or other outside computer facility	(205)

19. A. Has conversion of records to computerized form led to detection and correction of factual errors which previously existed in manual records? (Please mark only one response).

Ø = 688 Yes (301) No (105) Do not know (73) Does not apply (47)

19. B. Were the corrections about items important in making decisions about the individuals on whom records are kept? (Please mark only one response).

Ø = 690

Yes, considerable importance	(52)
Yes, marginal importance	(122)
No, of little importance	(122)
Do not know	(50)
Does not apply	(178)

19. C. Have there been significant problems in maintaining the accuracy of computerized records, which were not present in the manual system? (Please mark only <u>one</u> response).

Ø = 685

Yes, significant problems	(25)
Yes, marginal problems	(123)
No, problems of little or no importance	(332)
Do not know	(22)
Does not apply	(28)

20. A. A number of measures have been proposed to prevent access to computerized records by unauthorized persons. Do you use any of the following? (Please mark one response in each row).

	Ø	Yes	No
20. A.1 Control of physical access (e.g. door locks, badges for access to computer room)	739	(343)	(132)
20. A.2 Hardware/software security measures (e.g. pass-words, terminal identification code, cryptographic encoding.	750	(180)	(283)
20. A.3 Personnel integrity checks (e.g. special investigations of operating personnel; bonded employees)	745	(197)	(271)
20. A.4 Audit logs or other data monitoring methods	754	(264)	(194)
20. A.5 Procedures and rules for disposal of data (e.g. destruction of print-out or tapes)	745	(323)	(147)
20. A.6 Other, please specify	950	(31)	(232)

20. B. How many high-speed remote terminals other than keyboard terminals (e.g. card readers) are used in your system? (Please mark only one response).

Ø = 743

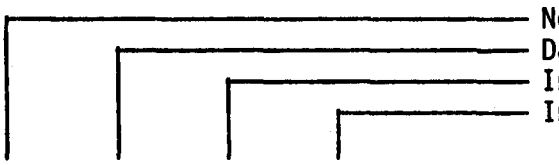
None	(348)	Over 6	(22)
1-6	(102)		

20. C. How many keyboarded remote terminals are used in your system? (Please mark only one response).

Ø = 743

None	(338)	12-200	(26)
1-12	(101)	Over 200	(7)

20. D. Please mark the statement which best characterizes your data processing operations with respect to remote access. (Please mark <u>one</u> response in <u>each row</u>).



20. D.1 Ø = 744	(353)	(10)	(5)	(103)	Remote high-speed terminals (e.g. card reader, printer)
20. D.2 Ø = 749	(352)	(18)	(15)	(81)	Remote keyboard terminals (e.g. teleprinters, video displays)

21. Does the application of computer technology in your organization enable you to pull together, in one record, all the information your organization collects and stores about a given individual?

Ø = 694 Yes (148) No (313) Does not apply (60)

22. A. Do you furnish more individually identifiable information about individuals to any government agency (federal, provincial, or local) as a result of increased retrieval capability after computerization?

Ø = 694 Yes (69) No (369) Does not apply (82)

22. B. Do you furnish more statistical (unidentifiable) information about individuals to any government agency as a result of increased retrieval capability after computerization?

Ø = 695 Yes (151) No (297) Does not apply (71)

SECTION 4

THE FOLLOWING QUESTIONS REFER TO COMPUTERIZED RECORDS IN THE FILE DESIGNATED IN THE COVER LETTER. IF YOU DO NOT USE A COMPUTER SYSTEM FOR THIS FILE, PLEASE STOP HERE AND RETURN THIS QUESTIONNAIRE TO US AT YOUR EARLIEST CONVENIENCE.

THANK YOU FOR YOUR CO-OPERATION

23. A For this file, are you collecting more data or less data on a given individual than before computerization? (Please mark only one response). Ø = 791

More data per individual is collected	(147)
About the same amount of data per individual is collected as before	(242)
Less data per individual is collected	(6)
No basis for comparison	(28)

23. B. Has computerization of these records directly affected the amount of data being collected per record? Ø = 791

Yes (158) No (247) Does not apply (19)

23. C. Which of the following conditions would you say is the primary reason for increased data collection? (Please mark only one response). Ø = 798

Increased collection, storage, and processing capability of the computer	(89)
Changes in organizational objectives or programmes or increasing government requirements for collecting or reporting information	(131)
Does not apply	(197)

24. A. With regard to the individuals on whom you maintain records in this file, do you maintain any other information in manual form on the same individuals?

Ø = 791 Yes (380) No (43)

24. B. How would you compare the information kept in manual form with the information in computerized form? (Please mark one response in each row).

	Ø	Yes	No
24. B.1 The more subjective (opinion based) information is still kept in manual form	824	(322)	(66)
24. B.2 The more narrative, lengthy or graphical information is still kept in manual form	817	(345)	(52)
24. B.3 The most sensitive and confidential information is kept in manual form	824	(294)	(97)

25. A. Have any new rules concerning the individual's privilege to examine his record in this file been issued since you began using a computerized record system?

Ø = 790 Yes (14) No (359) Does not apply (52)

25. B. Do you see this change as being a direct result of computerization of the records?

Ø = 792 Yes (11) No (69) Does not apply (343)

26. Are additional users under consideration for personal information in this file (e.g. sale of mailing lists, preparation of market estimates, etc.)

Ø = 796 Yes (81) No (336)

Please specify additional uses under consideration.

THANK YOU FOR YOUR CO-OPERATION. PLEASE RETURN THE QUESTIONNAIRE IN THE ENVELOPE PROVIDED.

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.