PRIVACY & COMPUTERS

A report by

Department of Communications/Department of Justice

PRIVACY AND COMPUTERS

2/PRIVACY AND COMPUTERS

1. Task Force on Privacy and Computers

A report of a Task Force established jointly by

Department of Communications/Department of Justice

Available by mail from Information Canada, Ottawa,
and at the following Information Canada bookshops:

HALIFAX
1735 Barrington Street

MONTREAL
1182 St. Catherine Street West

OTTAWA
171 Slater Street

TORONTO
221 Yonge Street

WINNIPEG
393 Portage Avenue

VANCOUVER
657 Granville Street

or through your bookseller

Price: $2.50 Catalogue No. Co21-3/1972

Price subject to change without notice

Information Canada
Ottawa, 1972

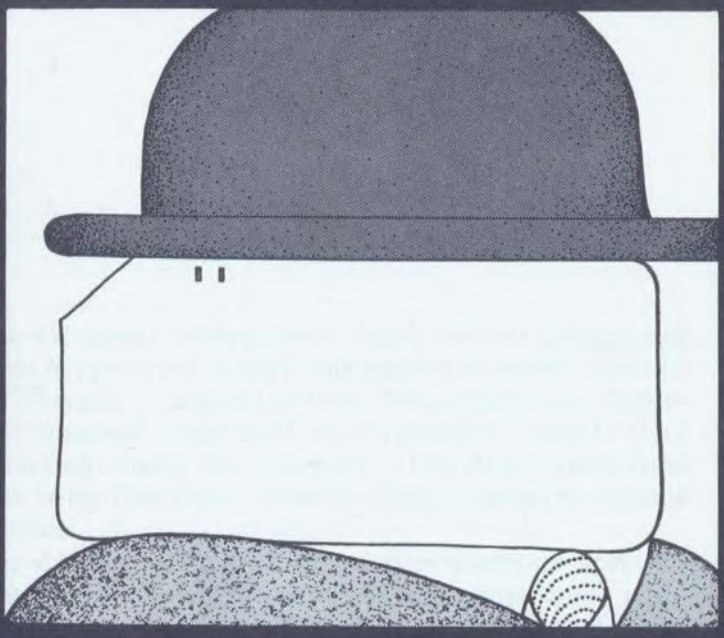
Design by John McIntyre
Hal Phillips

NOTE

This Report has been written by members of the federal Departments of Communications and of Justice on the basis of material compiled by expert consultants. The views expressed therein do not necessarily represent the policy of the Canadian government and no inference of a commitment to particular course of action should be drawn from the Report.

TABLE OF CONTENTS

Introduction



Introduction

The widespread development of highly efficient computerized databanks has given rise to increasing concern about their potential use for invasions of personal privacy. This prompted the Departments of Communications and Justice to establish, in April 1971, a Task Force on Privacy and Computers.[1] This Report summarizes the work of the Task Force; its terms of reference can be found in the Appendix.

The simplest explanation for the current concern about the relationship between individual privacy and computerized information systems is also the most obvious. The complexity of society coupled with the rising expectations of individuals and groups has led to increasing demands for information, both personal and impersonal. Since the advent of computers, with their associated memories, personal information has been collected and centralized to a degree formerly impossible. A hundred years ago, almost everyone was relatively unknown except in his own immediate neighbourhood. Today comprehensive personal details about everyone are stored in an ever-growing number of files, from education to credit, from welfare to insurance, from taxation to criminal history. By almost every act, from acquiring a passport to buying a car, each citizen leaves a trail of data behind; the volume of data increases from birth to death, and grows ever more comprehensive.

Concern about this uninterrupted growth in the accumulation

and distribution of data is of recent origin. In the United States it can be traced back to the 1965 hearings of the House of Representatives into a proposal, subsequently rejected, to establish a national databank. In Canada, no similar dramatic event has yet served as a focus for public attention. From time to time there have been expressions of concern: the press has paid increasing attention to the subject and there have been several debates in legislatures, commonly on the introduction of a bill by a private member. In May 1970, a conference jointly sponsored by the federal Departments of Justice and Communications and the Canadian Information Processing Society was held at Queen's University on the topic "Computers: Privacy and Freedom of Information".[2] The Privacy and Computers Task Force had its origin in the deliberations of that conference.

Today, study groups are wrestling with the issue in many countries, notably in Britain, France, the United States, the Federal Republic of Germany, (where the State of Hessen has enacted the first specific laws to regulate databanks) and Sweden (where concern about individual privacy is beginning to modify a long-standing tradition of freedom of information). Of special interest to the Task Force has been the comprehensive study of the issue undertaken by the National Academy of Sciences in the United States under the direction of Professor Alan Westin. There has been close liaison between the two groups throughout the study.[3]

The Task Force proceeded on the assumption that a study of privacy and computers was timely, and that this particular form of inquiry, by persons with expert knowledge rather than through public hearings, was the most effective method of tackling an issue of which the extent and exact nature was virtually unknown. Because of time limitations, the conceptual study, which attempted to come to grips with the value of privacy to society and to the individual, proceeded in parallel with rather than ahead of the other studies, which were primarily factual and legal. Both appraisals were essential for the advancement of a debate that had thus far dealt largely with philosophical abstractions and anecdotes of mishandled data.

The work of the Task Force was divided into 10 major study areas: a multi-dimensional exploration of the nature of privacy; empirical studies of the information-processing practices of government agencies, public institutions, and private companies; long-range technological developments; statistical databanks; security problems and safeguards; the judicial process; administrative or

regulatory remedies; self-regulatory remedies; constitutional considerations; and international considerations. The Studies commissioned by the Task Force, and their authors, are listed in the Appendix.

The picture of data-handling practices that emerged was revealing. No single organization yielded startling results, but the over-all synthesis revealed a network of information paths linking the bureaucratic structures, both public and private. In brief, more personal information is being collected than most Canadians probably suspect, and is made available to a larger number of users than is probably supposed. There is no evidence that either of these trends will decline.

The issues surrounding privacy and information can be separated into two fairly distinct levels. At the first level are specific concerns relating to accuracy of information, right of access to files, control of dissemination, security standards and similar matters. By and large, these issues require no fundamental conceptual analysis but rather a careful assessment of the precise extent and nature of the problems and possible solutions. For example, most people would agree that, in almost all conceivable situations, personal information recorded in files should be accurate, and that the individual should, to the greatest possible extent, know the purposes for which this information is being collected. Debate really begins with the delineation of specific abuses of such generally accepted principles, and of legislative or other actions which could or should be taken to prevent their occurrence.

At the second level are the more general and less tangible questions, such as: what is the relationship between information, privacy and political power? Will current and projected uses of the computer lead to loss of individuality or to enforced conformity? Is the desire for informational privacy fundamentally social or anti-social? How can a balance be achieved between claims to personal privacy and claims, as legitimate but sometimes conflicting, for unimpeded access to information?

The empirical data obtained and the legal analysis undertaken by the Task Force primarily address first-level issues. In the empirical studies the Task Force attempted to learn about the types of personal data collected about Canadians, the systems in which these data are stored, and the practices and procedures of the databank operators. On the legal side, it sought to ascertain the nature and extent to which Canadian courts and legislatures have responded to individual claims to personal privacy, and to examine a variety of means by which additional protection of personal

privacy might be afforded. Discussion of the more fundamental "second level" issues is much more tentative. On neither level was the Task Force called upon – nor did it purport – to recommend definitive solutions to particular problems.

Throughout the "computers-and-privacy" debate, it has been usual, over the past few years, to characterize as "privacy" values the array of individual interests, claims and values affected by the intensifying accumulation and handling of data. In this Report an attempt has been made to provide a certain measure of conceptual clarification by distinguishing between those values, interests and claims which may properly be regarded as pertaining to privacy as such, and those which, although equally or even more urgent, relate to other values such as personal reputation. At the same time, in any consideration of the most effective possible responses to the specific problems posed by the gathering and handling of information, the distinction becomes less relevant. These responses will have to be matched against the full array of actual and potential harms caused to individuals by the operation of databanks, regardless of whether these harms relate to privacy or to other values or rights.

If the "computers-and-privacy" debate comprises broader questions than privacy, it also encompasses far more than computers. As replies to the Task Force questionnaire revealed, about three-quarters of today's computerized files containing personal data are buttressed by manual files which, by and large, contain the more sensitive and subjective information. Nevertheless, it is probable that advances in technology will lead to the computerization of the great bulk of most types of information. Throughout this Report, therefore, the term "information systems" is used to encompass both automated and manual systems.

A final explanatory note about the scope of this Report is needed. A Task Force is a modish way of describing a study team, which in this instance was composed of officials and independent expert consultants. Their mandate was to describe and to analyze the present and likely future state of Canadian information systems containing personal data about identifiable individuals, and to examine various possible safeguards for personal privacy and related values. Thus, although the Task Force heard about or read reports in the media on alleged invasions of privacy, it did not examine their validity.

Those involved in the Task Force were:
Executive Committee:
A. E. Gotlieb, Deputy Minister, Communications
G.V. La Forest, Q.C., Assistant Deputy Attorney-General, Justice,
R.J. Gwyn, Director-General, Socio-Economic Planning, Communications
E. R. Olson, Q.C., Director, Legal Research and Planning, Justice

Co-Directors:
R.J. Gwyn, E. R. Olson

Principal departmental representatives:
Ann Johnstone (Justice)
K. Katz (Communications)

Consultants:
J. Baudot, Université de Montréal
J. Boucher, Université de Montréal
J. Carroll, University of Western Ontario
C.M. Dalfen (Director, Legal Services, Department of Communications)
C. Fabien, Université de Montréal
H.S. Gellman, President, DCF Systems Ltd., Toronto
C.C. Gotlieb, University of Toronto
P. Hume, University of Toronto
F.J.E. Jordan, Department of Justice
Carol Kirsh, Consultant, Toronto
J. Madden, Canadian Computer/Communications Task Force
J. Sharp, University of Manitoba
S. Usprich, University of Western Ontario
P. Vivian, University of Western Ontario
D. Weisstub, York University
J. Williams, University of Alberta
J.I. Williams, University of Western Ontario

Co-ordinating Editor:
C.M. Dalfen

Editors:
Ann Johnstone, J. Madden

French Editor:
F. Doré

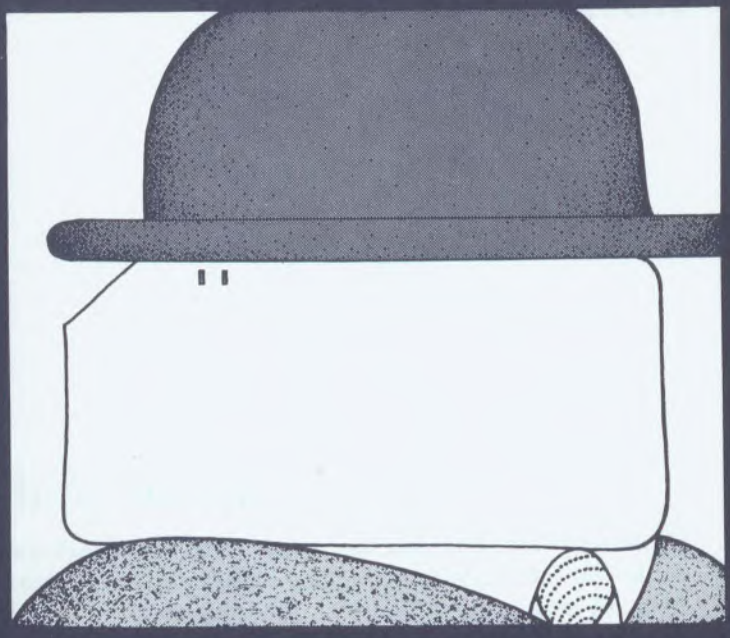
Production Editor:
Bette Byers.

[1] The issue of privacy was included originally in the terms of reference of the Computer/Communications Task Force which was established November 1, 1970, and which published its report August 3, 1972. Subsequently it was determined that consideration of a subject of such breadth and complexity required the formation of a separate study group.

[2] The report of the conference (Telecommission Study 5(b)) was published by Information Canada in May 1971.

[3] For a list of "parallel" studies being undertaken in other countries, see the Appendix.

Section I



Dimensions of the Issue

Chapter 1
Privacy and Information

1. Information

Since the advent of the industrial age, and to a dramatically increasing extent in the more complex post-industrial period, information of all types has been used and is being used for planning, research, and operations by government, business, universities, and virtually all sectors of society. Individuals, groups, and associations gather up information from the past, from abroad, from each other. Information is constantly being fed into their systems, processed, and then disseminated. It is often cycled and recycled. The appetite is a hardy one: the omnivorous data-gathering process churns relentlessly on.

The computer is a device in the service of the information process. It permits enormous increases over the capacity of manual systems in the quantities of data that can be processed, collated, stored, and retrieved. It centralizes this information in electronic databanks. It surpasses human memory by permitting the instantaneous retrieval of countless diverse facts. New systems with ultra-large memories are capable of storing over 100 billion characters at a cost of about one cent for 1,000 characters. Processing techniques

for handling such large stores of data efficiently are currently being developed. Related technological innovations are producing advances in user-oriented terminals, in more flexible and more comprehensive software packages, and in extending the power of computers through communications networks. In short, the capacity of computerized systems to provide information with unparallelled speed and efficiency will continue to develop in geometric progression.

What all this means is that there are great benefits to be derived from these information-processing systems, in terms of effective planning, resource allocation, and greater efficiency in various types of human activity. Almost every activity, from measuring the extent of pollution to administering a welfare program, depends upon a foundation of accurate, accessible information about both things and people. Without information, political debate and analysis is emasculated: information may "prove", or "disprove" that a particular institution discriminates against women in its hiring policies, that too many young people are chasing too few jobs, that old people are not being provided with adequate medical care.

The enormous technological capabilities of computerized information systems can, however, raise certain threats to important human values – like privacy – which are integral to our very conceptions of what it is to be human.

Society is coming quickly to recognize and to profit from the more obvious benefits of automated information systems if one can judge from the exponential growth of computers of all types. Society, however, is less aware and less clear about their possible threat to human values. The Task Force accordingly tried to focus on these values and the impact on them of computerized information systems.

2. Privacy in a Universe of Social Values

There is much confusion about the concept of privacy, which involves a variety of complex and often emotional issues. The term "*right* of privacy" is often used, although there is no clear legal or even social definition of such a right, and discussion of the subject inevitably uncovers both congruence and conflicts with concepts such as liberty, trust, power, and freedom of access to information.

Privacy is not a single value, claim, or interest. It is a constellation of values, claims and interests in a universe of concurring and competing values, of supporting and antagonistic claims, of allied and adverse interests. It is, moreover, a constellation changing over time and from culture to culture in a universe of different civilizations, societies, groups, and values.

What clearly appears is the highly individualistic nature of the claim to privacy. In organic societies like those of the Middle Ages, where primary emphasis was placed on social cohesion and the needs of the community, individual claims to stand apart were largely denied except to hermits, monks, or mystics. A claim to an identity independent of manor, guild, or church would have been antisocial if not heretical. In the rural and agricultural environment that characterized North America until fairly recently, a demand for isolation, beyond that imposed by the nature of the environment and the pattern of existence, would probably have been regarded as eccentric or even inimical to society and dangerous in times of emergency. At the same time these rural societies were characterized by a voracious appetite for gossip, and "secrets" about anyone were often known to all.

Thus, the claim to privacy, as we know it, is eminently a phenomenon of the industrial and post-industrial age, in which the exigencies of urban life have led to an atomic concept of society in place of the earlier organic model. Formerly, in moving from the country to the city, physical solitude was traded for anonymity; the exhange is increasingly nullified as anonymity is compromised by the spread of information systems and networks, while solitude in cities has been largely lost. Moreover, the process is one-way; institutions learn more about individuals, but individuals learn no more about the institutions, or even about what the institutions learn about them.

In any society, claims to privacy are continually balanced against other values and interests by social, political and legal processes. The security and welfare of the collectivity and its institutions are values which tend to prevail over individual claims to privacy. Similarly the demands of the state for revenue and its effective collection outweigh individual claims to refuse information about personal income. The degree to which different privacy claims are acknowledged in any given society varies with the predominant ideology and politics of the time. At any one time, certain claims to privacy may be legally supported (e.g., the right to privacy with respect to many activities in one's own home); others may be the subject of public and official debate, though not yet

legally enforceable; while still others may be regarded as unacceptable (e.g., a claim to keep personal-income data from the knowledge of the government).

Nor do all the claims made in the name of privacy fall clearly within the range of values and interests encompassed by any reasonable concept of privacy, however emotionally relevant some of them may be. Thus, the demand for access to personal information purveyed to others is more probably an attempt to secure a different distribution of political power (by neutralizing the impact of potentially harmful information) or a protest (against bigness, technocracy, impersonality) than a claim to privacy. And arguments about untrue facts being purveyed are not, strictly speaking, arguments about privacy but rather about defamation and other threats to reputation.

Nevertheless, despite the fluidity of values, the shifts of interest and the flux of claims, it is possible to identify a number of stable components of the privacy constellation, and to ascertain the general characteristics of the values that people seek to protect when they allege that their privacy has been invaded.

3. The Concept of Privacy

Privacy claims appear to fall roughly into three major categories, relating to property, to the person, and to information. What runs through all three, and is indeed the force attracting them into one constellation, is the fundamental principle that there are realms – in a physical and in a psychological sense – in which an individual may, as an attribute of his personality, demand to be let alone to do as he sees fit. This notion of a right to be let alone perhaps can be justified in terms of the uses an individual may make of his privacy, to enjoy other liberties, to fulfil other human needs, or to achieve desirable social goals. But that is not the point. What is essential is that these zones or realms of privacy are important, if not essential, for the well-being of the individual (and ultimately for the good order of the society), irrespective of what he may do within them. The very essence of a totalitarian society is that it penetrates and intrudes into these realms – with nearly perfect totality in Orwell's *1984*.

a. Territorial Privacy

Claims to privacy advanced in a territorial or spatial sense are related historically, legally and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquility is advanced and is recognized. A man's home is his castle. At home he may not be disturbed by trespassers, noxious odours, loud noises, or peeping Toms. No one may enter without his permission, except by lawful warrant.

b. Privacy of the Person

In a second sense, a claim to the privacy of one's person is protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person. This notion, like the territorial one, is spatial in the sense that the physical person is deemed to be surrounded by a bubble or aura protecting him from physical harassment. But, unlike physical property, this "personal space" is not bounded by real walls and fences, but by legal norms and social values. Furthermore, this sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. Our persons are protected not so much against the physical search (the law gives physical protection in other ways) as against the indignity of the search, its invasion of the person in a moral sense.

c. Privacy in the Information Context

The third category of claims to privacy was of primary relevance to the Task Force. It is based essentially on a notion of the dignity and integrity of the individual, and on their relationship to information about him.

This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. And this is so whether or not the information is subsequently communicated accurately, and whether or not it is potentially damaging to his reputation, his pocket-book, or his prospects; the context is of course the controlling factor in determining whether or not particular information will be damaging. Competing social values may require that an individual disclose certain information to particular authorities under certain circumstances (e.g., census information). He may decide to make it available in order to obtain certain

benefits (e.g., credit information or information imparted to his lawyer to win a lawsuit or to his confessor to win salvation). He may also share it quite willingly with his intimates. Nevertheless, he has a basic and continuing interest in what happens to this information, and in controlling access to it.

An individual has an interest, beyond the original access of another person to any particular fact about him, in whether and how it is further disseminated to third and fourth parties and to the public at large. This is particularly relevant where information about an individual is generated not by himself but by others, for example, his passport or car-licence number. In these cases the issuing authority is obviously in control of the information, but the individual also has a continuing interest in controlling its further dissemination.

Again, conceptually, the validity of this interest in controlling access to personal information is not derived from any mental distress or pecuniary harm that its dissemination or publication may cause to the individual concerned. His privacy is "invaded" as each new person becomes privy to the information. As more and more information about him, his "vital statistics", his personal habits and circumstances, becomes known to more and more people beyond his control, his personal autonomy is that much weakened, his personality that much more in the social marketplace, his privacy that much more invaded. Thus the privacy claim of an individual is also a claim not to have information about him pried loose (for example, by forced searches or confessions), gathered without his knowledge (as by wiretapping or eavesdropping), published without his authorization, or even conveyed to third parties without his consent.

For analytical purposes, there are thus two phases at which invasions of privacy may occur. The first is when a fact about someone is first learned by another – when it passes from the first person into the knowledge of a second. There would be, however, no "invasion" where this information is imparted voluntarily, for example to one's spouse, or to one's lawyer or confessor under the umbrella of confidentiality. There must be a type of wrongful prying. The second phase occurs when information is passed on to a third party or is made public. Again, however, there is no "invasion" if consent is given and the information has been freely given in the knowledge that it may be published.

4. Information Systems and Privacy Claims

The two phases at which privacy is brought into play in the operation of information systems correspond to identifiable stages in the information process. At the data-gathering stage, organizations attempt to learn potentially valuable facts about individuals. This is the first cognitive or fact-learning phase, even if the organizations glean this information at second-hand, as from gossipy neighbours, and are therefore, strictly speaking, the recipients of disseminated data. When these organizations in turn disseminate this information or pass it along intentionally or indirectly to other parties, the second phase of potential invasion of privacy occurs, as when these systems "leak" information through inadequate security techniques and procedures. There are widely varying opinions about the legitimacy of the different privacy interests and claims that may arise during both phases of the information process. The law, partly or wholly, recognizes a few of these claims. The Radio Act, for example, protects against the use and divulgence of information obtained through the unauthorized tapping of radio signals, and legislation prohibiting wiretapping was submitted to Parliament early in 1972. A far greater number of claims, however, are being advanced, and in some cases publicly debated, while others have not yet even been articulated.

Beyond the issues linked directly to privacy, information systems raise a large number of important related issues. While these arise irrespective of whether the systems are automated or manual, computers – by their speed, storage capacity and almost infallible memory – may magnify, or at least highlight the problems. The computer, which can be accessed through communications links, is a device whereby records about individuals (in varying but almost limitless quantities) can be stored, retrieved and passed on to others, often without the consent or knowledge of the subject; where disparate bits of information can be centralized, correlated, and reorganized in possibly damaging ways; where mistakes can be compounded and their effects exacerbated; where the fallibilities of human memory are no longer a source of relief. Privacy-related questions are thus brought into play, and are intensified as the number of files on individuals grows constantly in a variety of fields from education to credit, from welfare to insurance, from taxation to criminal history.

The Task Force attempted to identify and examine the activities and practices of data processors that seemed to threaten or bear on personal privacy and related issues. At the computer storage and processing stage, it considered the nature and types of data stored; whether the data were reorganized, merged, cross-referenced; the degree to which the accuracy of the stored data was ensured; the nature and extent of data-security; the extent to which individuals had knowledge of and access to the fact that information about them was being stored; and the extent to which individuals might know the contents of files of which they are the subjects.

In the data-dissemination stage, the Task Force examined the questions of who received what data, under what conditions, and with what knowledge, if any, on the part of the subject individual.

In addition to these empirical enquiries, the Task Force considered certain normative questions arising out of the information process. The following questions, among others, were specifically addressed:

1. Under what conditions should an individual have access to files containing information about him?
2. What rights should he have to delete, amend, or add to such files?
3. To what extent can it reasonably be required that personal data should be protected against intrusion or accidental disclosure?
4. What rights does the individual have regarding dissemination of information in his files? Should he be informed before such dissemination takes place, or be advised (by means of an audit) of all uses?
5. What responsibilities does a record-keeping organization have with respect to the merging and dissemination of personal data?
6. Should individuals be concerned about personal data concerning them which is held in foreign databanks beyond the territorial jurisdiction of Canada?
7. To what extent should an organization holding personal data be responsible for its accuracy?
8. Should there be conventions or rules concerning the types of personal data which specific organizations may or may not hold in their files?

Information systems – computerized or not – cannot themselves invade personal privacy, but their use almost inevitably entails it. The Task Force attempted to discern the extent of such invasion, its acceptable limits in view of conflicting demands for

increased knowledge and efficiency, and the safeguards to which individuals may reasonably be entitled in the development and operation of computerized information systems.

5. The Human Need for Privacy

The question whether there is a "basic human need" for privacy has been addressed by a number of authors. Westin in his book *Privacy and Freedom* investigated behavioural and anthropological writings in search of a natural or hereditary source of such a need. The evidence uncovered is convincing insofar as a need for spatial privacy is concerned, but less conclusive as regards informational privacy.

The territorial instincts of the animal kingdom have their parallel in the development of feudal domains and in the development of the law as it concerns the individual's person and property. In terms of survival of the species, there are rational explanations for territorial instincts. However, as regards the "territoriality" of information, anthropological studies of different tribes and civilizations have revealed a variety of customs and practices. Even in our own western civilizations we have the example of Sweden which, by law, provides that almost all government files are open to the public, including all income tax returns, while other countries, including Canada, prescribe stiff penalties for disclosure of the same information except in narrowly defined circumstances.

A variety of customs reflecting constantly changing situations and traditions within different societies suggests that one must enquire more deeply into human and societal relationships to find the roots of this repeated demand for informational privacy.

Westin, in his analysis of the human need for privacy, identified four distinct facets. These were *solitude* – to permit man to reflect on his experiences; *intimacy* – with family and friends to permit deeper, more meaningful relationships; *anonymity* – to permit him to exist outside the bounds of his historical development; and *reserve* – to permit him to withdraw from communications when he feels the need.

Of the four, it is anonymity that is most seriously undermined by a lack of informational privacy. But the word anonymity does not completely describe the human need to retain control of facts about oneself for release on a restricted and selective basis. Such behaviour might more nearly be described as a condition of partial reserve, in which a part of oneself is withheld from communication. This need in turn is almost certainly founded in a desire to be

able to impress people, in a controlled way, with a carefully tailored set of personal information. For certain friends and total strangers this façade may be lowered from time to time, but the desire for partial anonymity is strong in most humans. One writer[1] summarized this need with these words:

> "Daily life is therefore sparked by a constant tension between sincerity and guile, between self-release and self-containment, between the impulse to embrace that which is public and the drive to escape the discomfort of group demands. Accordingly, our identities are maintained by our ability to hold back as well as to affiliate."

In a world of total social cohesion and mutual trust, privacy might be unnecessary. Where there is no antagonism, total happiness is achieved through a total harmony of parts. In *Brave New World,* Aldous Huxley portrayed one vision of that utopia. Harmony and happiness were abundant, but somehow an important dimension was missing. The individual had lost his chance to make a wrong decision in a programmed world, and with that loss went a loss of identity, of individuality.

Related to this is the threat to individuality posed by the very concentration and processing of large quantities of data about individuals. This threat is one of conformist behaviour induced by the certainty that one's file exists and grows, coupled with the uncertainty as to what it contains and the uses to which it will be put. As Westin has expressed it:

> "public awareness of potential use would lead to an 'increase in behavior for the record' and less freedom of action and expression. People will be concerned not only with the fact that they are going 'on record', but also with how the record will look to those in authority..."

6. The Computer and Power

Apart from the individual values at stake, and apart from the direct terms of reference of the Task Force, computers raise important political issues about which public debate has only just begun. The computer has become not only a tool to assist man in processing masses of information, but also a device which may concentrate massive power in the hands of those who operate and control information systems. It can be particularly potent in the hands of large bureaucracies, both public and private. As Michael Harrington[2] has put it:

> "Bureaucracy is the only way to coordinate the complex

> functions of a modern economy and society and therefore cannot be dismissed with a curse. Yet it is also an enormous potential source of arbitrary, impersonal power which folds, bends, spindles and mutilates individuals but keeps IBM cards immaculate."

While computers can deal only with recorded information, and have not yet learned how to invade a person's mind and his innermost thoughts, this does not mean that they will never outstep the bounds of recorded personal information. It seems likely that researchers will develop techniques of producing a "psychological profile" of individuals by collating information on reading habits, family background, education, etc., along lines similar to the "profile" of a typical airplane hijacker used by airlines' personnel.

Science fiction literature abounds in stories of computers which exeeed human intelligence and manage to take over the world. Less dramatic but equally spine-chilling are the stories which portray men using computers to monitor all human activities, both physical and mental, and employing this information subtly or unsubtly to manipulate and exploit their fellow men.

The common element in these stories is the linkage of computers and power. It is fear of this new element in the traditional and better known power structure that is the mainspring of much of the concern for privacy. The invention of computers gives rise in our time to a situation somewhat analogous to the discovery of iron in prehistoric times, for as the weapons fashioned of the new metal must have been a key element in the ancient power structures so the computer's ability to store, manipulate, and transmit data makes it a key component of power today. Indeed, some writers view the question of informational privacy as being, in essence, a political and not a legal issue. Progressively, institutions possess more and more information about individuals, while there is little reciprocal flow of information about the institutions back to the individuals.

The computer, however, can be used both to concentrate and to disseminate information, and hence can be used to redistribute information (and in this sense, power) from organizations to individuals. For while it is not possible for a person to carry on more than one conversation at once, the computer can not only provide many people with simultaneous access to the same body of information but it can also accept simultaneous feedback from many people on a variety of issues. Coincidentally, it is also capable of limiting access to particular files or parts of files only to authorized enquirers. Furthermore, because computerization of files normally leads to centralization, it is easier to institute and police controls on

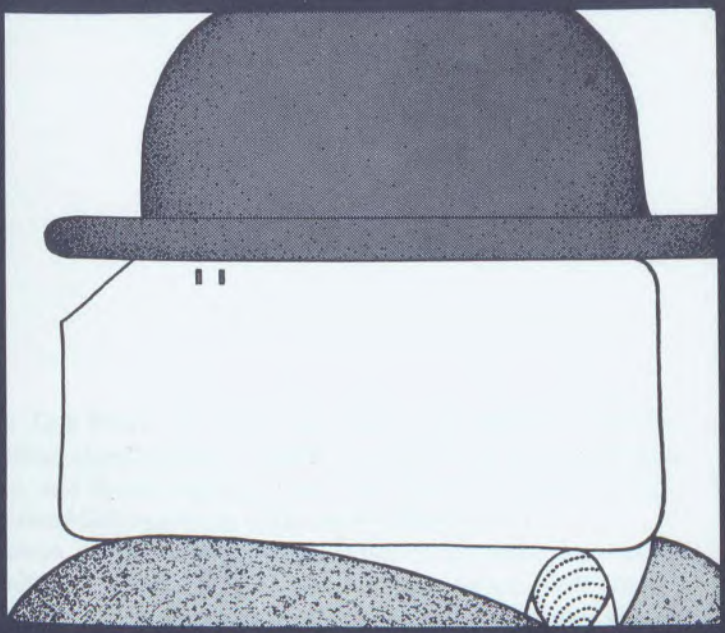
the handling of computerized personal information – though also easier, of course, to abuse the opportunities provided for central control.

Provided the political will exists, the computer can be a most effective instrument for achieving the dispersal of information, and therefore, to the extent that the two are linked, for the dispersal of power. Like any powerful implement, the computer can be exploited for good or for evil. The public will, rightly, cease to hold the computer in awe only when it will clearly be used solely as a power for good. Although its influence appears to have been largely beneficial so far, in terms of enhancing productivity and efficient administration, the issue of its full social impact is far from settled.

[1] Schwartz, Barry, "The Social Psychology of Privacy", *American Journal of Sociology,* May 1968, p.752.

[2] Michael Harrington, as quoted in Miller, Arthur, *The Assault on Privacy,* Ann Arbor: University of Michigan Press, 1971, p. 258.

Section II



Empirical Findings

Background

The Task Force devoted a large part of its effort to collecting information about current Canadian practices in the acquisition, handling, and dissemination of personal data, and about the attitudes of databank operators to the data in their care.

Because of the enormous quantities of personal data which exist, such an inquiry could at best be only partial. Furthermore, the survey in effect produced a snapshot picture (incomplete as it is) of the situation in 1971. Practices and opinions change quickly, so that care must be exercised in extrapolating to the future. Despite these hazards and short-comings, it is clear that some information carefully used is better than none, and even a hazy snapshot is a valuable aid in determining the best course for the future.

Discussion of the data collected has been broken into six parts. In Chapter 2, the method of data collection and some general conclusions will be presented. As has already been said, however, the diversity of requirements and practices means that general conclusions are necessarily limited in scope. In the next four chapters, information on data handling by specific organizations or groups is discussed under the general headings of statistical data-processors, administrative data-processors, including financial and medical data-processors, and investigative data-processors. Categorization of this nature is not all-embracing, and some liberties have

been taken in assigning organizations to one of the three groups. The final chapter in this section presents some information on the issue of whether or not there should be a single identifying number for each individual.

No attempt has been made to achieve a narrowly objective presentation. Where observations on data-handling procedures seem appropriate, they have been made. Information on foreign-held databanks has been incorporated under the appropriate organizational heading (e.g., credit, insurance) rather than as a coherent group of data (which it certainly is not). Where it seemed to be of more general interest, some aspects have been presented in more detail than would have been justified if the goal had been to produce a balanced picture of databank operations. For example, the problem of inadvertent statistical disclosure, a hazard peculiar to statisticians, has been treated as a separate sub-section in Chapter 3.

Except where annotated, the bulk of the material in this section is drawn from the Study prepared for the Task Force by Prof. J. Carroll, entitled *Personal Records: Procedures, Practices and Problems.*

Chapter 2
Information Systems: An Overview

1. Information Sources

The Task Force adopted several different methods of assembling the information it needed.

a. Questionnaire

Replies to a questionnaire provided the primary source of factual information on current attitudes and practices in the handling of personal data in Canada. This detailed questionnaire (see Appendix) was sent to 2,516 Canadian organizations thought to maintain large files of personal information. The mailing list was compiled from lists of the largest Canadian industrial and financial organizations, from the membership lists of associations in fields such as education, welfare, insurance, health services and organized labour, and from the current census of computers in Canada compiled by the Canadian Information Processing Society. The mailing list was deliberately designed to include not only computer users, but also organizations currently processing files manually.

The questionnaire was developed after consultation with Professor Westin who, at that time, was just starting to get replies

from the questionnaire he had distributed in connection with the study by the National Academy of Sciences in the United States. The survey questions can be divided into three general categories, namely:

- requests for factual information, such as the activities of the organization, the size and composition of its files, and the characteristics of its computing equipment;
- questions regarding current practices and experience in the handling of the data, and the existence of implicit or explicit procedures or policies;
- questions relating to attitude and perception, such as reaction to possible regulations and codes of ethics, the perceived need for such steps, and the need for various approaches to the provision of security.

Approximately 50% (1,268) of the questionnaires were returned completed. In addition, nearly 200 organizations wrote to explain why they had not returned the questionnaire – the most common reasons given were lack of knowledge and lack of time. The majority of those not replying were small companies or regional associations. Fewer than 100 operators of large information systems failed to reply. The organizations which did reply employed about 1.2 million persons in total, or about one-sixth of the Canadian labour force. Almost half the responses were from the public sector, primarily government agencies at federal, provincial, or municipal levels; the remainder came from the private sector. A classification of responses according to the function of the respondent organization is shown in Table 1.

Respondents were asked to reply to a particular set of questions directed at a particular class of file (such as employee, credit, etc.). The files studied (with the percentage of responses) can be roughly categorized as follows:

Employee	25.4%
Credit	20.8%
Health	14.7%
Welfare	7.4%
Education	6.0%
Insurance	6.0%
Enforcement	1.7%
Other	18.0%
	100.0%

In general, a good sample of large holders of personal data was obtained. Extreme caution is required, however, in drawing

Table 1

Questionnaire Respondents Categorized by Function of Organization*

	Replies	Non-Replies	Total Mailed
Banking, lending and other financial institutions	61	49	110
Life, accident, or casualty insurance	76	41	117
Public utilities	38	6	44
Publishing and mass communications media	8	17	25
Health or vital statistics	182	183	365
Education	76	45	121
Taxation	2	14	16
Driver licensing or auto registration	2	0	2
General merchandizing	22	21	43
Travel and entertainment cards or reservations	1	1	2
Oil company	22	7	29
Investment service	64	120	184
Law enforcement, probation, parole	11	4	15
Social Welfare or benefits	39	8	47
Chattel mortgage registration	1	0	1
Credit information exchange	10	16	26
Service industry	83	111	194
Major industrial employer	127	84	211
Regulatory agency	7	9	16
Employment agency	11	27	38
Market research	1	0	1
Associations (labour, professional)	95	337	432
Charitable organization	54	50	104
Mailing-list supplier	2	4	6
Private investigator, collection agency, insurance adjuster, etc.	43	68	111
Other	198	0	198
Question not answered	36	0	36
TOTALS	1272	1222	2494

*The exact wording of the question was:—

"How do you characterize the prime function of your organization?" Please mark only <u>one</u> category.

Response was better than 50% in most categories. The only significant body of non respondents was associations, principally local groups whose national body had replied or filed a brief, and district labour councils. Many taxation authorities (municipalities etc.) appear to have placed themselves in the "other" category.

general conclusions from such a disparate body of respondents. Not only is there an enormous diversity of function and interest, but the aggregations are such as to give the same statistical weighting to the responses of a large provincial health scheme as to a private company employing 20 people. The data thus have more relevance when the responses are considered in functional groups and related to the other information assembled by the Task Force.

b. Site Interviews

In order to provide a check on the validity of questionnaire returns and to familiarize members of the Task Force with the day-to-day problems faced by databank operators, a series of site interviews was arranged with 43 organizations. In selecting candidates for site interviews, an attempt was made to provide regional as well as occupational representation. Small as well as large organizations were included on the list. Each site was visited by two to four people; there was always at least one lawyer and one computer scientist present.

The interviews provided a valuable fund of background material on the actual operational problems and procedures of the organizations visited. The Task Force is indebted to the many individuals in those organizations who sacrificed significant amounts of time to provide information to Task Force members.

c. Briefs

Some 187 associations were notified of the existence of the Task Force and asked to submit briefs, or to solicit briefs from their members, if they were interested in making their views known. In selecting associations to receive the notice, it was decided that the better policy was to distribute it widely and expect a low response, rather than to mail only to those who had a clearly expressed interest in privacy. The response rate was indeed low: 16 briefs were received, but those that did respond provided some invaluable information.

In addition to the briefs submitted directly, Task Force members also had access to briefs submitted to the Computer/Communications Task Force, with which there was a close working relationship. Of the total of 200 briefs received by the latter, 54 referred to the need for privacy and confidentiality of personal information, and 22 of these made specific comments or recommendations on the subject.

d. Miscellaneous Sources

As well as the major data-gathering activities described above, there were several supplementary data sources, including the responses of 13 United States corporations known to store personal data on Canadian residents, to which enquiries were sent about their data-handling practices (for the list of respondents see the Appendix); the report of a computer attitudinal survey carried out across Canada by the Social Survey Research Centre under contract to the Department of Communications and undertaken independently from the work of the Task Force; and miscellaneous studies indirectly connected with the Task Force.

2. Information Systems and Personal Data

a. Summary of Findings

While much of the data collected was relevant only when viewed in the context of particular organizational groups, since results averaged over different groups often become meaningless owing to their disparate interests and behaviour, nevertheless certain broad conclusions can be given about the ways in which personal data are handled:

1. There is probably more data interchange than is generally realized by the public. Information networks flourish in many situations where the exchange of personal data is beneficial to both parties involved. Because of the informality of the process, precise description of the data paths is practically impossible, though questionnaire returns did yield some information on the networks. To a greater or lesser extent, police, credit-reporting agencies, insurance companies, educational authorities, and welfare agencies are (amongst other categories) involved in such exchanges, which usually take place without the person involved being informed of the activity. While many organizations, particularly the large ones, have written security and disclosure policies, there is a substantial body of hearsay evidence to indicate that these rules are often forgotten when communications with

persons who can be trusted to handle the information discreetly are involved.

2. A particular focus of concern appears to be the collection and use of information by governments. Of special significance is the fact that concern about government information-systems was frequently expressed by government officials.

   In a brief to the Computer/Communications Task Force, the provincially-owned Newfoundland and Labrador Computer Service Centre stated "Governments are potentially the biggest misusers of information collected on citizens... (Governments) should first articulate policies to prevent this."

   The federal Department of Manpower and Immigration in its brief focussed on a particular characteristic of public data-banks: "There will be a natural tendency (justifiably motivated by efficiency) to integrate the data banks with similar banks of other departments, provincial governments, civic welfare departments and possibly even some private agencies. While there will be a tremendous improvement in the effectiveness of social services, we may also experience a considerable erosion of privacy ... it is recommended that this aspect of integrated data banks be subject to some very specific policy guidelines." Similar sentiments were voiced by the New Brunswick Government and by several other departments of the federal government.

3. There was little fundamental difference in data-handling practices between governmental and non-governmental organizations. However, major differences in practices and attitudes were apparent when organizations were grouped according to function, such as credit, medicine, research, investigation.

4. The computer, as yet, plays only a limited role in the handling of sensitive, personal data, but that role is swiftly becoming more important. A typical computerized file today contains 1,000 to 5,000 records, each containing about 300 characters, and each processed 10 to 20 times a year. Decreasing costs are likely to make increasingly economic the computerization of less used, smaller files. Rising labour costs

and the increasing complexity of the social and economic structure are likely to spawn data-hungry computerized "management information systems"[1] in organizations of all shapes and sizes.

5. There are more inaccuracies in personal information systems than is probably generally realized. Seventy-five per cent of respondents to the question on the subject reported discovering mistakes in their manual files when these were automated. In the United States, in a field where accuracy would be expected, the conversion of a police information-system from print to machine-readable form disclosed errors in nearly one-third of the files. Because of data interchange, an error in one file can reappear in several other files.
6. Most information systems are still local in a formal sense but, through information interchange agreements, they are capable of operating on a national or international scale. However, organizations that are national or international in scope are rapidly introducing information systems commensurate with their geographical spread.
7. A survey commissioned by the Department of Communications[2] revealed that more than one-third of Canadians appear to believe that computers threaten their personal privacy, while more than half believe that computers will violate confidentiality. Although the vagueness of the terms "privacy" and "confidentiality" (which were not further defined by the survey) doubtless led to some confusion, the general degree of concern is significant.
8. By their apparent readiness, as shown in replies to the questionnaire, to accept some form of regulatory controls, databank proprietors, and more particularly the proprietors of large personal databanks, showed considerable awareness of and sensitivity to the issue of informational privacy.

   This general response, however, masks a wide divergence of views. Several organizations, such as the Canadian Book Publishers' Council and the Canadian Bankers' Association, took the view that the "need to know" is a more important value than unspecified invasions of privacy. Other groups, such

as the Canadian Manufacturers' Association and the Retail Credit Company of Canada, argued that legislation to protect privacy was either unnecessary or premature.

Other general observations that can be made about the operating practices and procedures of Canadian information systems are set out below:

b. State of Computerization

Whether or not personal records are stored in computerized databanks depends upon several factors such as the technological sophistication of the agency, its capital position, its management policy, the frequency with which its files are consulted or updated, and the number of active records and their structure.

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

About half the respondents to the questionnaire used electronic data-processing, and of these about two-thirds operated their own computers. The remainder used computer service bureaux. About half the computer users made their first use of computers in the period 1965-69. The rate of initiation of organizations to computer use fell off sharply after 1969, an indication that the electronic data-processing (EDP) industry has reached a degree of maturity. However, a significant decrease in the rate of installation of new computers came to light, indicating that existing users are continuing to improve their facilities. This finding is borne out by the analysis of the EDP industry undertaken by the Computer/Communications Task Force, which has estimated a cumulative growth rate of approximately 17% per annum for the 1970's.

Slightly more than half of those having computerized files felt that, while the computer provided a useful improvement, they could continue operations without it: about 10% believed that the computer had had little or no impact on their use of files. Only 40% said they could not continue operations without the computer.

It would appear that in many cases computerized records

supplement rather than supplant the old paper files. Ninety per cent of those maintaining computerized files also indicated that they maintained other information in manual form on the same individuals. Furthermore, over three-quarters of those maintaining personal files replied that the most sensitive and confidential information was kept in documentary form. This revelation clearly emphasizes the importance of the problem of informational privacy in a context broader than that encompassed by the computer alone.

Of those owning computers, 32% replied that their computers allowed them to pull together into a single record all the information possessed by the organization about a single individual, but only 16% replied that the advent of the computer had directly resulted in more individually identifiable information about people being furnished to government. Just under 40% thought that the advent of the computer had directly resulted in more data per individual being collected; the rest noticed little change. Only 3% of those replying indicated that computerization had directly resulted in new rules concerning the individual's privilege to examine his record.

c. Security Standards and Practices

Security and privacy are often confused. The former (as it relates to this study) describes the degree of protection afforded to personal data, whereas the latter is a legal and social concept of some complexity (as discussed in Chapter 1). Wherever an objective is to restrict access to personal data to authorized viewers, some security procedures must be introduced. A consideration of security provisions and attitudes is thus necessary to any practical study of informational privacy. There are often several motives other than the protection of personal privacy which reinforce the desire of organizations to make their databanks secure. These include concern for the privacy of many business and government transactions, and, particularly as regards computerized records, fears of physical assault or sabotage.

Statistics on security procedures are not very meaningful when averaged over all Canadian systems. A few averages do, however, help to provide a general background. Twenty-three per cent of respondents thought it unnecessary to police the actions of their staff with regard to misuse of personal information. Of the remainder who did monitor staff activity, one in eight claimed to have actually caught offenders, and to have prosecuted or disciplined

them. More non-profit than profit-making organizations fell into this last category. About three-quarters of respondents operating computers have controls over physical access to the equipment, and about 40% have implemented hardware or software security measures such as passwords, terminal identification coding, or cryptographic coding. A similar percentage run personal integrity checks on data-processing personnel, and over two-thirds employ secure disposal methods for unwanted data tapes or printouts.

In response to the question "Is there a general management policy regarding disclosure of personally identified information?", one-third responded that they had a written policy, 55% had an unwritten policy, and the remainder replied that no policy had been formulated. As is to be expected, the large, more technically sophisticated, organizations generally paid more attention to security. Clients and customers were about two and a half times more likely to benefit from a written disclosure policy than employees, although the latter did benefit from an unwritten policy in 70% of organizations, and were protected by a non-disclosure policy in 14% of the responding organizations.

d. The Exchange of Information

From the responses to some questions, it was possible to trace several data-exchange paths between organizations with differing functions. Not surprisingly, the groupings followed logical patterns, although those who had not previously considered the subject may have been unaware of the extent of some linkages. For example, private conversations with an insurance agent in British Columbia revealed that personal, financial, and behavioural information was quite readily available to those who are known in the information exchange network, while a British study on the Right of Privacy[3] reported that agencies in the United Kingdom offer personal bank-balance information for sale at about $16 a record, while unlisted telephone numbers can be obtained for just over $10.

Organizations most likely to use investigators to gather personal data are law-enforcement agencies and insurance companies. Social welfare agencies, regulatory agencies, merchandizing houses, and major industrial employers (in descending order) also make significant use of investigative credit bureaux and private investigators. Educational and medical organizations are extensively used as sources of personal information, as is a person's employer.

As noted, most information systems are local in a formal sense, but through information interchange agreements they are able to conduct operations on a national or international scale. Forty-eight per cent of respondents indicated that they furnish personal data to recipients in the United States. The types of organization most likely to do so are credit bureaux, regulatory agencies, law-enforcement agencies, large industrial employers, insurance companies, merchandizing houses, and employment agencies. Both of the mailing-list suppliers and motor-vehicle bureaux which responded said they furnished data to recipients in the United States. Fifty-nine per cent of respondents say they obtain personal data from suppliers in the United States.

e. Record Purging

Over half the respondents retained records on individuals after their relationships with the organization had been severed for more then seven years. Less than 15% purged their records in the first 18 months after the relationship had terminated. About two-thirds of those which purged files destroyed them. All the rest transferred them to inactive files or archives, except for four organizations (less than half of one per cent) who returned the files to the individuals concerned.

f. Location of Files

Only five responding organizations said they had all their files in the United States, and four of these were labour unions. Sixty-six per cent of all files containing personal data are located within the particular province in which the organization operates. Twenty-six per cent of the files are located elsewhere within Canada. Eight per cent are wholly or partially in the United States; among them (aside from labour unions) were oil companies, insurance companies, health services, and lending institutions. Almost half of all respondents with some files in the United States were incorporated in a foreign country.

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

g. Complaints

Recipients of the questionnaire were asked "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?" Seventy-five per cent of respondents replied that no such complaints had ever been received, and a further 15% either did not know or said the question did not apply. Of those who admitted receiving complaints, 10% (121) received them only occasionally. Only four respondents received frequent complaints. Although four is hardly a valid statistical sample, it is perhaps of some interest that two of these respondents were hospitals and the other two were investigative agencies.

Acknowledged complaints about methods of collecting personal data were in about the same proportion as acknowledged complaints about information disclosure. Only five organizations reported frequent complaints, of which three were in the insurance or insurance-adjustment business.

About 16% of respondents replied that individuals (or groups representing an individual's interests) occasionally sought to examine their own records or complained about the organization's practices regarding the permissibility of examining their record. Less than one per cent (mostly hospitals) said this occurred frequently, while the remainder either said there was no demand by individuals to see their record, or were unaware of any such demand.

Of those who had converted personal files to computer-readable form, about three-quarters of those prepared to give a "yes" or "no" answer admitted that the conversion had led to the detection and correction of factual errors. Thirteen per cent felt that the errors uncovered were of "considerable importance", and a further 30% felt the errors were of "marginal importance". These figures provide some indication of the probable accuracy of most files.

The experience of a Canadian life-insurance company which converted data on several hundred thousand policies from punched card to magnetic tape storage several years ago provides an interesting footnote. They uncovered an average of one error per policy, an occurrence which so took them by surprise that their whole conversion program had to be delayed for two years while the data were verified and corrected. The 33% error encountered during the computerization of police records in the United States has already been mentioned.

In the survey of Canadian attitudes towards computers undertaken by the Social Survey Research Centre on behalf of the Department of Communications, about 30% of those surveyed reported that they or someone in their immediate family had "had trouble with errors in bills, subscriptions, credit, etc. due to computer errors."

h. Attitudes and Perceptions

As is to be expected, attitudes towards privacy and perceptions of issues vary substantially according to the functions of the organizations with which individual respondents were associated. A policeman who daily sees criminals using every possible legal angle to avoid arrest or conviction is unlikely to be as concerned about personal privacy as the Chief Statistician of Canada who, as well as being legally obliged to protect privacy, also knows that her sources of reliable statistics would dry up if leaks developed.

The questionnaire contained a series of attitudinal questions essentially in the form of statements enunciating positions on various issues concerned with privacy, asking whether the respondent strongly agreed, agreed, was neutral, disagreed, or strongly disagreed. The results have been charted in Figure 1. Where a particular organizational group differed from the commonly expressed attitude, this has been noted in the comments column.

Statements on which there was common agreement with no significant dissention on a group basis were:

- subjects of records containing personally identifiable information should have the right to correct, rebut, update and expunge incorrect or obsolete information;
- standards of security should be required for personal databanks;
- standards for the acquisition and dissemination of information should be adopted;
- files should be purged periodically of obsolete information.

Somewhat surprisingly there was strong over-all agreement with the idea that databank proprietors and information brokers or suppliers should be licensed. Only the organizational groups comprising publishers and mass communications media (seven responses in total) disagreed strongly as a group. Their sentiments may have sprung from a concern for the traditional freedom of the press.

The pattern of responses to the idea that databanks should be registered, as to purpose and content, was consistent with the responses on licensing of databank employees.

The right to be informed of the existence of personal records when they are started drew strong support, although the credit bureaux, for reasons which will be discussed in Chapter 4, registered strong disagreement as a group.

The concept of a right to review one's personal file on demand was more controversial. Law-enforcement agencies, regulatory agencies, insurance companies, and health-services organizations all registered disapproval. This response is in apparent contradiction to the almost unanimous agreement that subjects should have the right to correct, rebut, update, or delete incorrect or obsolete information. It can only be surmised that those dissenting from a right to review one's personal file had not fully considered the implications of an affirmative vote for the right to amend incorrect information.

The following three hypothesized rights met with no clear agreement or disagreement:

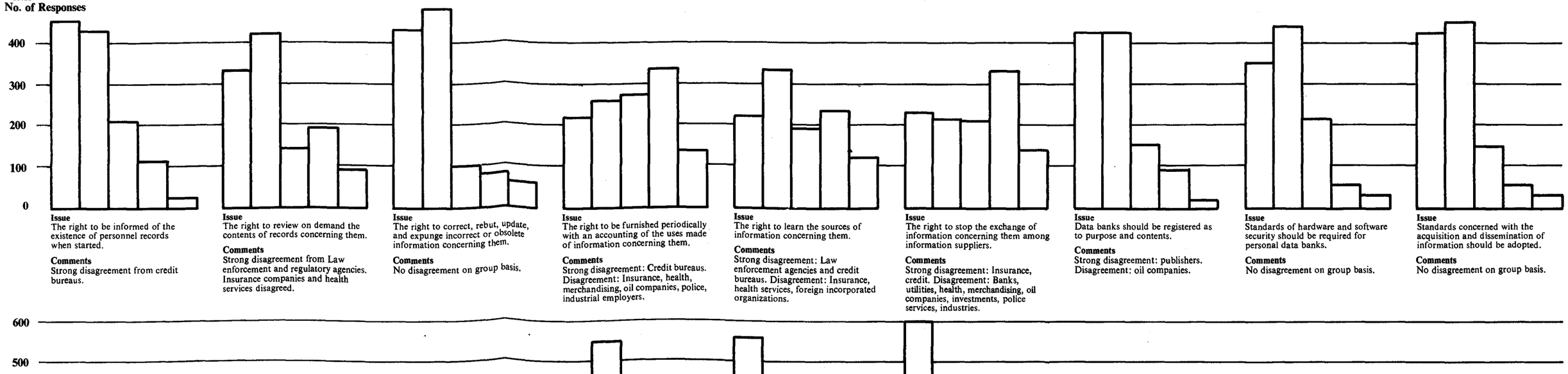
- the right of an individual to be furnished periodically with an accounting of the uses made of information about him;
- the right of an individual to learn the sources of information about him;
- the right of an individual to stop the exchange of information about him among information suppliers.

Likewise there was no clear consensus as to whether information-system proprietors should furnish personal data to law-enforcement officers on demand. The idea that records are the exclusive property of the information-system proprietors, and that subject-individuals have no justifiable interest in the files, was generally repudiated, although credit bureaux and merchandizing houses agreed with the statement, as did a number of other respondents.

3. Classification of Databanks

In the light of the information collected, and for the purposes of later discussion, it is useful to define three broad categories of personal databanks: statistical, administrative, and intelligence. This categorization allows the following distinguishing features to be highlighted:

Attitudes as Derived from Questionnaire Results



Issue
The right to be informed of the existence of personnel records when started.

Comments
Strong disagreement from credit bureaus.

Issue
The right to review on demand the contents of records concerning them.

Comments
Strong disagreement from Law enforcement and regulatory agencies. Insurance companies and health services disagreed.

Issue
The right to correct, rebut, update, and expunge incorrect or obsolete information concerning them.

Comments
No disagreement on group basis.

Issue
The right to be furnished periodically with an accounting of the uses made of information concerning them.

Comments
Strong disagreement: Credit bureaus. Disagreement: Insurance, health, merchandising, oil companies, police, industrial employers.

Issue
The right to learn the sources of information concerning them.

Comments
Strong disagreement: Law enforcement agencies and credit bureaus. Disagreement: Insurance, health services, foreign incorporated organizations.

Issue
The right to stop the exchange of information concerning them among information suppliers.

Comments
Strong disagreement: Insurance, credit. Disagreement: Banks, utilities, health, merchandising, oil companies, investments, police services, industries.

Issue
Data banks should be registered as to purpose and contents.

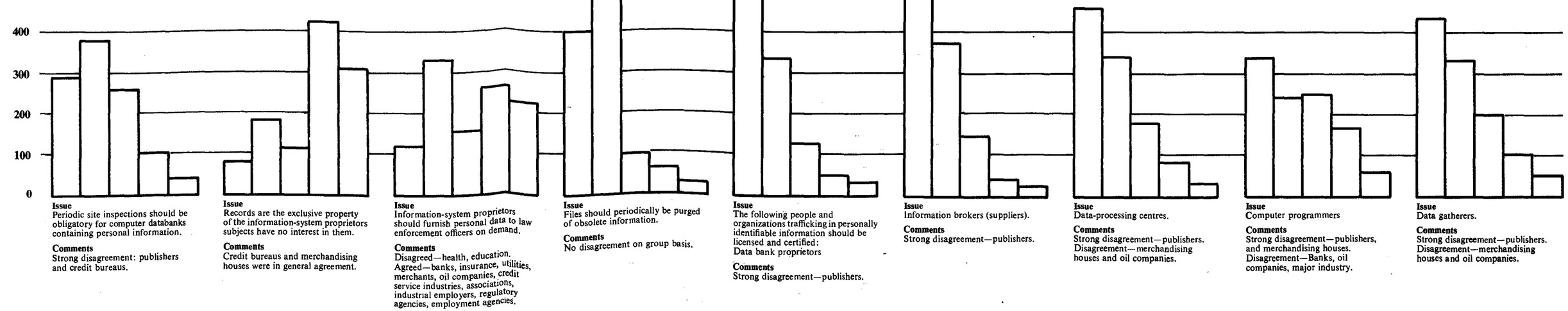
Comments
Strong disagreement: publishers. Disagreement: oil companies.

Issue
Standards of hardware and software security should be required for personal data banks.

Comments
No disagreement on group basis.

Issue
Standards concerned with the acquisition and dissemination of information should be adopted.

Comments
No disagreement on group basis.



Issue
Periodic site inspections should be obligatory for computer databanks containing personal information.

Comments
Strong disagreement: publishers and credit bureaus.

Issue
Records are the exclusive property of the information-system proprietors subjects have no interest in them.

Comments
Credit bureaus and merchandising houses were in general agreement.

Issue
Information-system proprietors should furnish personal data to law enforcement officers on demand.

Comments
Disagreed—health, education.
Agreed—banks, insurance, utilities, merchants, oil companies, credit service industries, associations, industrial employers, regulatory agencies, employment agencies.

Issue
Files should periodically be purged of obsolete information.

Comments
No disagreement on group basis.

Issue
The following people and organizations trafficking in personally identifiable information should be licensed and certified:
Data bank proprietors

Comments
Strong disagreement—publishers.

Issue
Information brokers (suppliers).

Comments
Strong disagreement—publishers.

Issue
Data-processing centres.

Comments
Strong disagreement—publishers. Disagreement—merchandising houses and oil companies.

Issue
Computer programmers

Comments
Strong disagreement—publishers, and merchandising houses. Disagreement—Banks, oil companies, major industry.

Issue
Data gatherers.

Comments
Strong disagreement—publishers. Disagreement—merchandising houses and oil companies.

Strongly agree | Agree | Neutral | Disagree | Strongly disagree

Statistical Databanks

- Data output is in aggregate form only. Individuals need not and should not be identifiable.
- Data input is often (but not always) personally identifiable, and is often stored in that way in order to permit statistical aggregation over many different variables.
- Data are wide-ranging and include most if not all categories of information that can be regarded as private.
- The databanks are often large, and in most cases they are highly amenable to the use of computers as an aid to sifting, sorting,and reducing the data.
- Quite aside from legal requirements, as in the case of Statistics Canada, there is usually strong motivation on the part of a statistical agency to protect sensitive data, since its ability to continue to collect accurate data is dependent on the extent to which it is trusted by those supplying the data. Some agencies, such as Statistics Canada, are required by law to protect the confidentiality of data.

Administrative Databanks

- Administrative data are essential to all organizations. There is a great variety in the volume, sensitivity, and purpose of the information gathered.
- Except for instances of gross abuse which lead to remedial action being taken, there is often little direct incentive to exercise particular care over the handling of personal data.
- In many instances (e.g., welfare, education employment), there is a dependent relationship between the administrator and the subject, so that the subject has little power to determine what information should be given or how it should subsequently be used.
- Administrative data in any one location are often potentially sensitive in only one or two areas at once; for example medical and income tax data do not normally coexist in the same file (except to the extent that the individual has claimed tax relief for medical expenses).
- Because administrative databanks often have parallel

interests (for example in the financial status of actual or potential clients), pressure exists for data exchange. Such exchange may occur on a formal basis, in order to achieve cost economies, especially when data records are owned by the same organization such as a government or a corporate conglomerate.
- Significant benefits to the individual often result from the existence of the files (e.g., driver's licence, welfare, employment), or from dissemination of the information they contain (e.g., credit as a result of information given by an employer, medical data disclosed in an emergency).

Intelligence Databanks

- Intelligence databanks usually exist because of actual or potential break down in trust between members of society Police intelligence files provide the most obvious example, but credit bureaux of the investigative type and private investigators compile files in the same category, primarily for potential employers and insurance companies.
- Information in the files is often comprehensive (i.e., it often includes criminal, medical, social, and financial data).
- Much of the information is, by its very nature, hearsay.
- The existence of the file (and of the investigation) is usually unknown to the person investigated.

[1] Management information systems can be loosely defined as systems designed to process and present data in such a way that it will provide managers with information pertinent and useful to the performance of their function. There has been much recent debate over the efficacy of computerized management information systems. Most of this has concerned their suitability to provide assistance for top level management (usually heavily involved in strategic planning activities). However management information systems are most likely to become intrusive when employed at a lower (administrative) level. Systems of this type appear to be well within today's capabilities.

[2] Study of public attitudes towards computers, undertaken independently from the Task Force activities, and conducted by the Social Survey Research Centre of Toronto for the Department of Communications. The study will be published in 1972.

[3] The Oxford Group of Labour Lawyers, "Report on the Right of Privacy", March 1971.

Chapter 3
The Statisticians

The struggle to improve our economic well-being, and the substantial successes achieved in this direction, have generated a voracious appetite in both the public and the private sectors for economic statistics of almost every imaginable kind. This hunger for data is not motivated by idle curiosity as to how the world looks, but represents an attempt to come to grips with the complex of demands, interests, and power structures which arises at least in part from the fact that our drive for economic efficiency has led us to become a community of specialists. With specialization has come a diversification of the power structure, a phenomenon which Drucker, in *The Age of Discontinuity*[1], called "the new pluralism". The very complexity of the economic system demands that intuition and good judgment be fortified and guided by statistical data. This is true both of governments, which must assess the need for new policies and the impact of the old ones, and of industry which must continually assess market needs in order to remain competitive.

The increasing realization that the old economic criteria for decision-making have somehow been inadequate measures of our progress has led to renewed demands for data of a much more wide ranging nature. Economics and nuclear physics have been displaced as fashionable topics for university study by sociology and computer science, and the combination of the latter and

related disciplines has spawned a multitude of "quantitative" studies attempting to bring order to our knowledge of human goals, behaviour, and attitudes.

Examples of the pervasiveness of social science research abound. An Eskimo delegate to a recent conference at Inuvik complained that "the average Eskimo family consists of a father, a mother, grand-parents, two children, a sociologist and an anthropologist."

While some would argue that collection of personal statistical data does not contribute directly to human well-being, it is difficult to envisage a recession in statistics-gathering without a simultaneous retreat to a less specialized, less economically efficient society. Whether or not such a retreat is desirable, or whether or not the right statistical information is being collected, is beyond the scope of the study, which proceeded on the assumption that for the foreseeable future the social structure would continue to become more complex, and that this trend would lead to increasing rather than decreasing demands for statistical data. Furthermore, research using statistics has demonstrably improved human well-being in many instances. The linkage of cigarette smoking with cancer by statistical reduction provides one well known example. Improvements in health care for the aged resulting from a statistical analysis of medicare records in a prairie province provide another; this particular study was conducted on an unofficial basis and without the knowledge, let alone approval, of the individuals affected, so that an invasion of privacy produced a clear benefit to those involved – one of the many examples of a cost-benefit trade-off.

Since a great deal of the data collected, be it economic or social, contains personal information, it is evident that the mere act of collecting the data must often involve invasions of privacy. At some point saturation is reached, although this may be constantly deferred as society is conditioned to accept the giving of data as a normal activity, and to regard the regular door-knock of a pollster as a welcome break from routine like that provided by Bible, Encyclopedia, and brush salesmen.

Indeed the Task Force itself contributed to the problem it was examining; the questionnaire survey resulted in a flood of statistical tabulations, while the study of public attitudes towards the computer undertaken by the Department of Communications gave rise to further probings and tabulations.

Aside from the issues of what, how much, and by what means data should be collected, the most important group characteristic of

statisticians is that they have a strong motivation to handle data under conditions of confidentiality, since their sources of information will evaporate unless confidentiality can be guaranteed. This characteristic is not universal. Researchers who do not plan to seek further information from an individual are free from many of the pressures towards a scrupulous respect for confidentiality. In the instance of market research firms, concern for privacy can be directed more towards their clients than towards the subjects of their interviews.

Given a general need or voluntary desire to ensure confidentiality, statisticians nevertheless face certain difficulties in its achievement.

1. Statistical Disclosure [2]

Several hypothetical situations exist in which inadvertent disclosure of personally identifiable information could result from manipulation of statistical data published in aggregate form. The simplest is accidental direct disclosure, which arises when an entry in a statistical table contains only one person or organization, or when there are several entries, but one of the persons or organizations completely dominates the total figure provided. I.P. Fellegi of Statistics Canada has undertaken an extensive investigation of this and other problems of a similar nature. He writes[3]:

> "It is a generally accepted practice to blank out information which is based on fewer than three respondents on the assumption that any two respondents of a particular kind might easily know of each other and hence, if a statistic based on two respondents were published then any one of the two could subtract his own report from the published aggregate and would thus deduce the quantity reported by the other. When there are more than three respondents but one or two respondents account for more than a specified proportion of the aggregrate the information is also blanked out. This is obviously necessary in the case of highly skewed distributions where the number of respondents by itself is hardly an appropriate guideline."

A more complicated problem is that of residual or complementary disclosure. Residual disclosure occurs when a set of tabulations can be manipulated arithmetically to yield, through deduction, information about an identifiable respondent, even though no single tabulation discloses such information. For example, residual

disclosure could occur if an entry in a table is blanked out but can be deduced from the marginal totals and the other entries in the table. Each time a new tabulation is produced from the same survey data, a new disclosure could occur through the arithmetic manipulation of the set of tabulations. It is necessary, therefore, to devise preventive methods.

While complicated theoretical solutions have been devised, the currently favoured approach is to introduce a minor level of random disturbance into every table. Such a system results in the "inoculation" of the collected data with random errors of which the statistical properties are known. This inoculation makes it impossible to obtain unambiguous information about a specific person even if identification is accomplished. This procedure, which is likely to be adopted by Statistics Canada, does add minor errors to the tabulation, but these errors are small compared to others that already exist.

2. Statistics Canada

The principal activity of Statistics Canada in terms of involvement with the population is the decennial census, with more limited data being collected at five-year intervals. The collection of individual census returns is governed by the Statistics Act, which provides that individual returns will be used only for statistical purposes and will not be made available for taxation or other administrative action; that the returns will be handled only by sworn staff of Statistics Canada; and that the data will be published only in a form which will not permit the identification of data relating to any individual, firm, or other respondent unless a specific request is made by the respondent. It can be argued that the existence of the comprehensive Statistics Act provides Canadians with greater privacy protection than U.S. citizens since no counterpart statute exists in the U.S.

Enumerators distribute census forms which, once returned, are checked and microfilmed as two distinct records. The first, which is destined for computer entry, contains names only in its microfilm form while the actual computer tape contains no names in machine-readable form. The second, a census search record, contains names, addresses and ages only (before the most recent census the complete record was stored). Once the microfilms are made the original forms are destroyed by shredding.

In addition to the census, Statistics Canada publishes annually 140,000 statistical series. Great care is taken with all personally

identifiable data: if some material has to be processed outside the institution, staff members transport the data and remain present during the processing.

Statistics Canada is unique among federal agencies, other than the Department of National Revenue, in that citizens have a statutory obligation to provide information, balanced by an equal obligation on the agency to ensure confidentiality. The relevant sections of the Act impose penalties on "Every person who, without lawful excuse, ... refuses or neglects to answer, or wilfully answers falsely, any question requisite for obtaining any information sought in respect to the objects of this Act" and at the same time requires that "no person other than a person employed or deemed to be employed under this Act, and sworn under section 6, shall be permitted to examine any identifiable individual return ... and no person who has been sworn under section 6 shall disclose or knowingly cause to be disclosed, by any means, any information obtained under this Act in such a manner that it is possible from any such disclosure to relate the particulars obtained from any individual return to any identifiable individual person, business or organization."

The remainder of the section lists the circumstances under which disclosure is permitted. Among these are: disclosure to a statistical agency of any of the provinces at the discretion of the Minister (and under strict non-disclosure conditions); disclosure when prior consent in writing has been given by the party concerned; and disclosure of information, other than personal data, which is public under statutory or other law.

All information obtained from other agencies is subject to the same secrecy requirements as those undertaken by the collecting agency. These secrecy requirements are so widely known that some farmers have listed marijuana in the "other crops" category, confident this information will not be passed beyond the walls of Statistics Canada.

Because of the large quantities of data involved and the extensive manipulation to which they must be subjected, Statistics Canada depends heavily on computers. Most data processing is carried out on an in-house computer, access to which is strictly controlled.

3. Social Science Research [4]

A general trend towards greater concentration of effort in research in the social sciences, buttressed by greater concentration on empirical studies, some of which involve statistical models requiring vast quantities of data, has hastened the establishment of the computer as an important tool for social scientists. Not only has there been an increase in the number of faculty and students in the social sciences gathering information for various educational reasons, but there has also been a dramatic change in methods of manipulating the information which is frequently transferred from the questionnaire to magnetic tape or some other type of plastic cartridge, microfilm, or microfiche. When stored in computer-legible format, the information is much easier to retrieve and correlate.

There is some concern for privacy in the social sciences over methods of data collection because a few researchers have resorted to questionable practices. Furthermore, much of the information collected by researchers is not only private in the generally accepted sense, but concerns extra-legal activities such as drug-taking or prostitution. Although the information is normally given on the understanding that it will be held in the strictest confidence, there is some question as to whether it might become available to law officers by subpoena. The American Council of Education has tackled this problem by identifying personal files with a code number only, and storing the linking file, which identifies names with code numbers, in a foreign country (Canada in this case), to ensure that its files cannot be effectively subpoenaed or seized.

Universities and research organizations generally are understandably reluctant to accept any controls imposed on them from outside. The alternative, self-regulation, is not widespread, although the Institute for Behavioural Research of York University has adopted an extensive code of ethics and is using security procedures similar to those used by Statistics Canada.

In July 1971, letters were sent by the Task Force to the chairmen of the sociology departments of a number of Canadian universities enquiring as to the existence or planned existence of ethics committees to oversee research on human subjects. The 18 replies revealed the existence of four such committees, one of which had jurisdiction only in the department of sociology. Four other universities were planning some action in this area. Reaction to the suggestion that ethics committees might be desirable ranged from warm endorsement to the statement that "As a researcher and

teacher of research methods I would be the first to object to the establishment of such a group."

In the United States, some measure of control is exerted by the Russell Sage Foundation, which provides substantial financial support to social science research. The Foundation insists that all recipients of its grants comply with its code of ethics, which includes provisions for the protection of personal privacy. Similar controls are not currently exerted in Canada, although an example could be set in federal funding of social research.

4. Market Research Firms

The Task Force planned, but for administrative reasons was unable, to interview a major market research company. The number of such companies responding to the questionnaire was too small to permit any generalizations to be made about their procedures and practices, although a consultant's report, without adducing concrete evidence, commented that standards of security become lower as one moves from government through universities to commercial market research firms. Such firms of course engage in far more than market research: their activities range from the ubiquitous political surveys, of which those by Gallup are regularly published, to attitudinal studies.

[1] Drucker, Peter F., *The Age of Discontinuity,* Harper and Row, New York, 1968, 383 pp.

[2] The discussion of statistical disclosure and of Statistics Canada is drawn largely from a study for the Task Force by H.S. Gellman entitled *Statistical Data Banks and Their Effects on Privacy.*

[3] Fellegi, I.P. "On the Question of Statistical Confidentiality", Proc. of the Social Statistics Section, American Statistical Association, 1970, p. 7.

[4] The discussion of social science research is drawn largely from a report prepared for the Department of Communications by T. McPhail entitled *Social Science Research and the Rights of Human Subjects.*

Chapter 4
The Administrators

Administrators comprise by far the largest class of users of personal information. Few administrators will go out of their way to obtain information which they do not believe to be relevant to decisions they have to make, but on the other hand there is not the incentive to protect the confidentiality of data which applies to the statisticians. Furthermore, an administrator will naturally look for the least complicated way of obtaining information. If the information he wants is likely to be embarrassing to the individual concerned, it is often easier to get it from anonymous sources, rather then let the individual know the extent of his probing. Mutual administrative convenience therefore leads to the formation of informal information exchange networks which permit network members to bypass regulations designed to protect confidential information. This type of bypassing reaches its most extreme form when a member of one organization is transferred to the payroll of another organization to provide a common point of data transfer between the two.

Another factor which tends to give administrators more freedom than might be desired is the effective power they exercise over the individual. This phenomenon is most apparent in relationships such as those between social workers and welfare recipients, and

between employers and employees, but in fact most people are unwilling to "rock the boat" even in much less sensitive matters.

This chapter and the next describe the standards and practices followed by administrators in a number of different areas.

1. Employers

Employers gather information about prospective employees to help them decide whom to hire. They continue to gather information to monitor employee performance, and to help decide whom to promote or dismiss. Records of former employees are often retained to administer superannuation benefits.

When an employer requires a check on a prospective employee, it is generally performed by an investigative reporting agency. The amount of information gathered about a prospective employee depends upon the importance of the position sought. During one site interview, a company manager said of the information collected on blue collar workers: "We just collect enough data on those fellows to pay them." Applicants for senior executive positions, on the other hand, are likely to be subjected to fairly thorough investigation and checking.

Information in even greater detail is required of persons in positions requiring a security clearance. Additional information in such instances often includes fingerprints, changes of address, and basic personal data on close relatives. In situations where national security is involved, this information provides the basis for an investigation by the Royal Canadian Mounted Police.

According to the questionnaire responses, about 40% of employee files containing 500 or fewer records are computerized, as against 76% of such files containing more than 500 records. The federal Public Service Commission maintains a voluntary on-line computerized inventory of skills known as Data Stream, which can be used by authorized personnel through 32 terminals located in various departments. Access is controlled by user identification and password, but no audit log is kept on who obtains what information for what purposes. Only 69,000 or 32% of federal public servants have files in the Data Stream databank. Those included are primarily in the administrative, professional, or semi-professional categories. Although basic data such as name, address, age, salary, and position are automatically included in the databank, the employee has a choice as to whether or not he wants his detailed employment history and list of skills recorded. Detailed on-line

personnel records like Data Stream are, however, the exception rather than the rule.

Most, though not all, employees have the right to see and rebut their records, although many employers made it clear that they would want to know why an employee wanted to examine his file before letting him do so. In the case of unionized employees, the terms of access and the nature of the information in the files are often governed by clauses in the collective agreement. In addition some employers have voluntarily stopped collecting information, such as that relating to national origin or religion, which might be used as a basis for discrimination.

Employers are one of the principal sources of information about individuals. Credit reporting agencies routinely seek information from employers, as do prospective new employers and educational institutions. Increasingly, employers are refusing to volunteer information other than to confirm or deny employment, unless a specific request for information-release by the employee has been made. However, as a matter of mutual interest, certain types of businesses, including banks, insurance companies, department stores, jewellers, and furriers tend to co-operate with police requests for information about employees.

Even the unemployed appear in computerized files. The federal Department of Manpower and Immigration is developing a system to maintain, in instantly retrievable form, a computer file of job seekers, with a description of their work history and job requirements. It is hoped that this file will greatly improve the ability of the Department to match job vacancies with those seeking employment.

2. Credit Granters

We live in an economy which depends heavily on the granting of credit for its proper operation. Although an evaluation and judgment of the societal effects of this situation, or of possible alternatives, is beyond the scope of this Report, there is certainly no sign of slackening in the move towards greater dependence on credit. The amount of consumer credit outstanding in Canada has multiplied by more than five in the past two decades, to some $9 billion in 1971. Types of credit include real-estate and chattel mortgages, small loans, bank cards, travel and entertainment cards, oil-company credit cards, and department-store charge accounts. Because of the dominant role played by the banks, they have been considered separately in the next chapter.

Taking the massive existence of a credit industry as self-evident, two of its characteristics were of particular interest to the Task Force. First, most of those who give credit endeavour to obtain detailed information about those who seek it before credit is granted. Second, individuals who consume on credit instead of using cash leave behind them a visible trail of purchases: evenings spent at a night club or hotel, trips out of town, money raised, or houses bought. Information is both the foundation of the credit industry and its principal by-product.

The search for credit involves a classic give and receive relationship. As the Royal Bank of Canada explained in its brief to 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.[1] Any information provided to a bank is regarded as 'privileged' between bank and customer. It is considered as the 'property' of the customer."

Some lenders make decisions regarding loan eligibility on the basis of information available within their own organizations, but most use the services of some outside agency. These outside agencies include in-file credit-reporting agencies, central registries of indebtedness, and credit-card monitoring services. Investigative credit-reporting agencies are used much less frequently.

Some provincial Attorneys-General have established computer-based systems for the registration of real and personal property and securities, primarily to prevent the fraudulent sale of property subject to liens. Most entries concern people buying cars on credit. Access is open to anyone willing to pay the fee of $2 per entry.

Small-loan companies maintain a lenders' information-exchange through the Canadian Consumer Loan Association, which maintains records on current debtors (to ensure that their credit limit is not exceeded), and on debt defaulters. The Credit Index, located in Morristown, New Jersey, and accessible by teletype, contains information on nine million people who have collectively defaulted on half a billion dollars of debt; 8,500 people in the index have Canadian addresses.

Banks generally rely on their own record of experience with particular customers in deciding on loan applications, although information from other bank managers, from credit bureaux, and from the customer's employer is not infrequently used. Banks have a strict policy of non-disclosure of customer-information except in well defined circumstances which can generally be categorized as

being either under compulsion of law or with the express or implied consent of the customer. However a bank will provide to a credit bureau, upon request, a credit reference with regard to unsecured personal loans. Such reports divulge the maximum credit, payment experience, existing loan position, and length of experience with the customer.

Under common law the relationship between a banker and his depositors is confidential, and the former may be sued for breach of confidentiality should he disclose the contents of the latter's account, although material damage must be proven before the individual can obtain a favourable judgment.

Credit-card operations such as Chargex, the oil-company credit cards, and American Express rely heavily on computers to provide up-to-date accounting information and to help prevent credit card frauds of various kinds. Many provide immediate access to computerized files by persons authorized to accept credit cards. The computer output normally provides information only as to whether or not credit is good, and whether or not the credit card has been stolen.

Many credit cards are accepted throughout North America, and the credit-checking system reflects this situation in that much of the data-processing for Canadian credit-card holders takes place in the United States. Thus information on many Canadian oil-company credit-card holders is stored in a computer owned by the National Data Corporation of Atlanta, Georgia, and is accessible through a terminal in Toronto.

American Express appears to maintain the largest credit data-bank on Canadians in the United States, with approximately 130,-000 Canadian credit card holders on file. Information is almost entirely of an accounting nature. Diners Club (with approximately 75,000 Canadian accounts), Carte Blanche (with about 14,000 Canadian subscribers) and American Airlines (with about 1,500 Canadian subscribers mostly in the Toronto area) run similar operations.

It has frequently been pointed out that extensive use of a credit card by an individual can result in his leaving a fairly complete record of his activities. This record can be useful to the police as well as to others. It is not unknown for criminals to be apprehended as a direct result of using a credit card.

3. Taxation

Many Canadians regard information about their income as highly personal and confidential, although others harbour no such feelings. Most Canadian wage-earners are obliged, however, to disclose their earnings to the tax collector.

The Department of National Revenue (Taxation Division) is responsible for the collection of federal individual and corporate income taxes, Canada Pension Plan contributions, and unemployment insurance premiums. The Department also collects provincial income tax for all provinces except Quebec. All staff must take an oath of secrecy, and are liable to "a fine not exceeding $1,000" for communication of tax return information to "a person not legally entitled thereto."

About 230 employees are engaged in data processing, supplemented by 1,000 temporary keypunch operators at peak-load periods. Tax returns are key-punched by both alphabetic (e.g., name and address) and numeric (e.g., taxes paid) units. The volume of production makes it virtually impossible for the operators to read anything except the data they are keypunching, or in fact to remember any of it.

Tax data are stored in several computerized files, the most important of which are:

- the master file of individual taxpayers, comprising 10,500,000 records of 500 characters each, stored on 125 reels of magnetic tape (the retention of three generations of back-up tapes permits the master file to be reconstructed in the event of accidental or deliberate erasure);
- the individual accounting and collection file containing up to 1,500,000 records of 400 characters each;
- the employer source-deduction file (500,000 records of 300 characters); and
- the T-4 supplementary-data file (15,000,000 records of 40 characters).

The principal recipients of tax-return data outside the Department of National Revenue (Taxation) are:

- Statistics Canada, which has access to corporate tax returns in order to carry out its obligations under the Corporations and Labour Unions Returns Act of 1965. It also has access to statistically selected samples of individual tax returns under the Statistics Act of 1971.

- Crown Attorneys when information is required to prosecute tax fraud.[2]
- The nine provinces for which taxes are collected. Quebec, which handles its own tax records, is able to use provincial tax returns for means testing and to verify statements of income made in support of applications for student awards. Officials claim this check saves the province $6 million a year in grants denied to ineligible applicants. The other nine provinces are denied this use of the tax data since the Income Tax Act allows it to be used for statistical purposes only.
- NR slips concerning United States residents are sent to the United States Internal Revenue Service in return for corresponding data concerning Canadian residents, in accordance with treaty obligations.
- A taxpayer may see his own return at the District Tax Office on proof of identity, and may give written authorization to an agent to see his return.

The Taxation Division is currently planning a remote-enquiry system which will permit data from the central tax base in Ottawa to be immediately available to any of its 28 district offices.

4. Life Insurance

Trying to cheat the insurance company seems to have been an international activity for at least 100 years, judging from the measures the companies take to protect themselves from inaccurate applications and fraudulent claims. Generally, insurance companies find it necessary to gather and use a great deal of information in the process of underwriting policies and adjudicating claims. This information is kept in manual form. Information for policy maintenance, such as premium payments and contract modifications, is often computerized. The industry was early to embrace the computer since its operations are frequently conducted on a large scale.

An applicant for life insurance relates information to the agent, which is then forwarded to the head office. An applicant is normally expected to provide a medical history and to sign a blanket release of medical information held about him by professionals or institutions. He may also have to undergo a physical examination, the report of which becomes part of his application.

The Medical Information Bureau (MIB) in Boston, Massachusetts, plays an important role in the search for fraudulent or high-risk applications. The MIB is an association of 700 life-insurance companies, of which 80 are Canadian. The Bureau's function is to alert insurers to hazards and impairments discovered by other insurers and not revealed by the applicant. When an insurer declines or reclassifies an applicant because of a serious ailment, a coded resumé is transmitted to the Bureau; the action taken by the company is not. Occasionally reports are made to the Bureau of favourable results of medical tests that may have future health significance.

However, any type of information may be the basis of a report to the Bureau. Although 90% of reports reflect coded medical information, 10% reflect non-medical information. The Bureau receives 1½ million reports from member companies annually (one Canadian company registers about 1,000 names a month) and answers 18½ million requests for information each year. According to information furnished to the Task Force by the Medical Information Bureau, the files contain information in coded form on 800,000 Canadian citizens or residents. These files are segregated from others kept by the Bureau.

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

The majority of 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 application for insurance. In fact, most Canadian applications for life insurance are accepted. A brief from the Canadian Life Insurance Association to the Task Force revealed that during 1969, 97% of applications for individual life insurance were accepted. About one per cent were rejected because of heart disorder, and slightly less than one per cent because of other serious health problems. Of the remainder, about one in fifteen rejections was because of dangerous occupation.

Applications for fire and car insurance also often result in

investigatory activity. The Fire Underwriters Investigation Bureau in Montreal maintains an index of fire insurance, burglary, and other loss claims. Motor vehicle bureaux will furnish transcripts of driver's records, including infractions and convictions, on request. In Manitoba the administrator of the provincial automobile insurance plan has the authority to gather any information he needs from government files.

5. Education

Except in Ontario, where a government bill on the subject has recently been introduced in the Legislature, there is little sign of explicit policy regarding the confidentiality of student records in Canada, yet the Task Force questionnaire revealed that over one-fifth of respondents received information about individuals from educational institutions.

A survey of Ontario universities conducted in 1970 revealed only two that had policies regarding the handling of student records.

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 regarded as 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 an exclusively confidential matter between the student and the faculty member directly concerned. In other institutions, marks lists may be circulated to all the 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 universities collecting information on race, religion, and national or socio-economic origins, for fear that these facts may be used to discriminate 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.

Documentation released outside a university consists in part of transcripts of academic records and letters of recommendation from the faculty. Transcripts are usually certified Xerox copies of a

permanent transcript card to which are affixed computer-produced labels giving course numbers, credit values, and marks. Many transcripts include a recapitulation of secondary-school marks. A transcript is released on request of the student and sent directly from the registrar to the employer or institution seeking it.

Record keeping for secondary and primary schools is likely to become computerized on a district basis. This task is made considerably more difficult by the fact that typical student records contain substantial personal information in free format inserted by counsellors. Much of this is eliminated by the computerization process.

The Ontario government introduced a bill in the Legislature in May 1972 which establishes the rights of students (and parents of students under 18) to have access to student records, and forbids access to the records by employers, police, and the courts.

There is substantial reason to believe that it is common practice for applicants and their families to understate income and resources when applying for student awards to provincial universities. Applications for student awards are often centralized at the provincial level where they are first checked by computer to see if eligibility criteria are met. Generally, income data is taken at face value in making the initial decision. A sample of the applications (sometimes as high as 25%) is normally extracted for special audit.

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, where, as already mentioned, it is estimated that $6 million per annum is saved by detection of fraudulent applications.

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 statement 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 parents' income, may be requested or balance sheets may be sought from chartered accountants in the case of fathers who are businessmen.

6. In-file Credit Bureaux

The term "credit bureau" is used to describe two businesses of different nature: investigative credit bureaux and in-file credit bureaux. The words "credit bureau" when applied to the investigative organizations are misleading, since their major customers

are not primarily the credit granters, but are more likely to be life, fire, or car-insurance companies, or prospective employers, although mortgage companies and travel-and-entertainment card granters are not infrequent users.

In-file credit bureaux do not normally become involved in investigative activities, but depend largely on information given to them by their customers, who are primarily department stores, small-loan companies, and small businesses which extend credit. To a lesser extent, the services are used by banks and oil companies. Although the in-file bureaux are not, strictly speaking, administrators, they do provide a kind of centralized administrative service, and for this reason they have been included in this chapter.

The in-file credit-bureau industry consists of a number of independent credit bureaux, most of which (151) belong to the Associated Credit Bureaus of Canada (ACB of C), a voluntary association. Over-all, it is estimated that the Canadian industry grosses $12-15 million annually, and employs about 2,000 people. The average charge for a credit report is $1.35.

Members of the ACB of C subscribe to a code of ethics, and to explicit policies to protect privacy. Many of the consumer rights provided for in the United States Fair Credit Reporting Act of 1970 are included in the code of ethics and associated policies. This is not altogether surprising in view of the links between the Associated Credit Bureaus Inc. in the United States and ACB of C. This linkage permits credit files to migrate with the individual almost anywhere in the United States and Canada.

Although no Canadian credit bureaux are yet computerized, the question is under serious consideration, since the bureaux are under strong pressure to provide more complete and up-to-date service. The principal obstacle to computerization is the high cost of conversion, a cost which is difficult to justify in relation to the relatively small volume of business. Several United States bureaux have already computerized their files (e.g., Credit Data, Retail Credit Corp.), and there is a possibility that the Canadian bureaux may want to rent a software system from a United States company and run it on a computer in Canada. Even with an imported software system, however, the file-conversion costs would be high. If the credit bureaux do not convert to computerized records, there is a danger that current customers will turn to other sources of information.

Retail Credit of Canada, a subsidiary of the Retail Credit Corporation of Atlanta, Georgia, which is primarily an investigative credit bureau, has been diversifying into in-file operations.

Approximately 30% of the in-file credit business in Canada is now under its control.

A common suggestion is that credit bureaux should be required to notify a person every time his file has been consulted. The credit bureaux oppose this on the grounds, first, that most people who apply for credit know that their file in the credit bureau is likely to be consulted, and second, that the extra cost would be prohibitive. Even a cost increase of 10% (or 14 cents per enquiry), it is argued, would be enough to affect business significantly, because many customers would start using the more expensive but more complete files of the investigative credit bureaux (about $5 per enquiry) or else start granting credit according to an arbitrary set of rules based on such criteria as age, occupation, and length of residence. They therefore concluded that the consumer would either be forced to pay a higher price for credit or be refused credit for arbitrary reasons.

This argument is worth noting. However, the contention that most people know, when they ask for credit, that a credit bureau file about them can be consulted is open to dispute. Even more open to dispute is the implication that they know how to go about finding their file if they should want to look at it.

It may well be expensive if credit bureaux are forced to alert an individual each time his file is consulted, but an obvious compromise would be an initial notification the first time the file is used (to alert the individual that his file exists), and the subsequent maintenance of a record of use which could be examined on request. Any right to examine the file should carry with it a corollary right to correct inaccuracies and include a procedure for resolving disputed facts. Members of the ACB of C do in fact permit inspection and correction of files by the individual concerned.

7. Mailing List Vendors

The question of commercial trafficking in mailing lists is on the periphery of the privacy issue, but it is nonetheless true that many people resent, and even regard as an invasion of privacy, being bombarded with "junk" mail simply because they have subscribed to some magazine, attended a conference, or registered a motor vehicle. On the other hand, for many others, particularly shut-ins, scanning of the "junk" mail provides a welcome diversion and a possible source of useful information.

Some provincial motor-vehicle licensing bureaux have made it

a practice over the years to sell a mailing list of licence holders at a cost of one cent a name. Manitoba has recently raised the price to 10 cents a name. Several provinces are reviewing the policy of selling the list in the light of mounting criticism.

Some business-magazine publishers have developed very refined mailing lists by adding to the basic subscriber-data, information obtained from mail-in reader-interest studies and responses to reader-inquiry services, which some professional associations have adopted similar tactics with respect to their membership lists.

Direct mail is normally only a minor irritant, but it can lead to some unfortunate consequences. In one such situation a young mother-to-be got onto a direct mailing list by virtue of pre-natal medical services she had received. Unfortunately she suffered a miscarriage, but was nonetheless the recipient of an eloquent congratulatory note from a bank at about the time the baby should have been born. Mailing lists for obscene literature are sometimes derived from improbable sources. One victim got listed by ordering a book on horse breeding from a publishers' clearing house.

In a letter published in the magazine *Computers and Automation,* Congressman Gallagher[3] quoted from a letter received by the San Francisco Suicide Prevention Service which read in part:

> "Dear Mr. Suicide: ... a subscription is one of the best ways to benefit the personal financial growth of the Suicide family."

He used this example of computer-generated "personalized" junk mail as a springboard to plead for adoption of his junk mail bill, which has four main provisions:

- register mailing list brokers;
- allow the individual to avoid receiving any unsolicited mass mailing, or any other than those relating to charitable, non-profit purposes;
- allow the individual to remove his name from specific lists;
- require every piece of unsolicited mail to contain identifying information clearly indicating where the sender obtained the name of the recipient.

The computer provides a relatively easy relief for those who do not want to receive junk mail. It is a simple matter for anyone to indicate whether or not he wants to receive such mail at the time the initial mailing is received – provided the form offers such an option. Once the data on the form has been fed into the computer, it is easy to provide mailing lists containing only the names of those who want to be included. This solution, which has already

been adopted by some organizations, should be satisfactory to all, in that the resultant mailing list is more valuable both to its owner and to those wishing to use it, since higher returns per advertising dollar can be expected.

[1] This need for personal financial information seems to be applied by several banks even when individuals obtain fully secured loans, a situation in which it would appear that possession of the security by the bank would obviate the necessity for any additional financial information.

[2] In a recent enquiry before the Exchequer Court, it came to light that tax information concerning a federal public servant had been made available to Crown Attorneys for reasons other than tax fraud. In giving his judgment, the judge specifically avoided comment on the legality of the information transfer on the grounds that such considerations were beyond the jurisdiction of his court, and the information so divulged was irrelevant to the judgment.

[3] Gallagher, Cornelius E., *Computers and Automation Vol. 20*, No. 4, April 1971, p. 35.

Chapter 5
The Bankers and the Doctors

The files of bankers and doctors are really only special cases of administrative files. However, in terms of the sensitivity of the personal information and more particularly of the impact of computer technology on the handling of that information, these two occupations are worth singling out for special consideration.

The problems faced by the two are, of course, very different. Medicine is facing a shift away from a personal doctor-patient relationship towards the health team approach to medical care. State-financed health care, with its enormous billing information systems, is also having an effect. Bankers are facing a squeeze of a different kind. The volume of paperwork is increasing at about seven per cent per annum while the staff that handle the paper are demanding and getting ever higher salaries. Banks are already heavily involved in computerization, and the trend is certain to intensify. At the present time they account for about seven per cent of all Canadian EDP expenditures.

1. The Bankers' Databanks [1]

At present, the most usual way to transfer money is through the use of bank cheques. In 1969, Canadians wrote 1.25 billion cheques, and the seven per cent growth rate is expected to continue until about 1980. It has been estimated that each cheque is handled an average of 14 times, at a processing cost to the bank of 13 cents. Significant cost reductions could, therefore, be achieved if the method of monetary exchange were simplified.

The banks have used computers during the past decade to speed up their processing of cheques. In Canada, automation in banking started in 1963 with the use of high-speed sorting machines and specially imprinted codes on cheques. These sorting machines read the codes, sort the cheques by account number, and feed the information (account number and amount) directly into a computer, which produces the customer's monthly bank statements.

At present, about 60% of the branches of Canadian chartered banks are using computers in the process described above. About 450 branches of Canadian chartered banks and trust companies use specially designed keyboard terminals connected to central computers by telephone lines to perform functions such as recording deposits and withdrawals and updating the customer's savings account record. The Bank of Montreal expects to have a comprehensive computer communications network connecting all its branches to a large-scale central computer facility before 1975. It is estimated that by 1977 up to 75% of all the branches of Canadian banks will be connected to on-line systems.

Computers have helped speed the movement of paper but have not reduced the amount of paper in the banking system. During the past 15 or 20 years, systems designers have been arguing that the best solution to the money transfer problem is to bring the computer right into the transaction. Paper could be eliminated entirely if terminals – all linked to bank computers – were installed in stores, homes, and offices. A transaction in this kind of system could involve merely the entry of information on the keyboard of a terminal or a Touch-Tone telephone.

The use of credit cards has received a lot of publicity. Many people have pointed to them as the harbingers of a chequeless society, though in fact they have been used principally as a substitute for cash, and have resulted in even more cheques and paper transactions. In the United States, the banking industry has predicted that in the next five years more than 40,000,000 people will be using bank credit cards to make $15 billion worth of purchases

each year. In Canada, by far the largest credit card system is Chargex, which had approximately 3.2 million card holders and a transaction volume of $302 million in 1971.

A recent article[2] described in colloquial language a version of the type of monetary system envisaged, perhaps within 20 years.

> "Joe Smith is travelling and needs some ready cash. He goes into a bank and presents an identification card (the only card he has to carry) to a teller, who puts the card into a terminal box. A green light appears. The teller punches a few buttons and hands Joe his money. Joe signs a receipt.
>
> Joe is not worried about the size of the balance in his bank account back home because the day before was payday, and his employer passed the funds through the wire transfer system to his bank...
>
> Let us examine Joe's card... There are several forms of identification on it. It carries the name of his bank and his identification number (each in both readable print and machine language); it also carries his signature and photograph and has an invisible (magnetically encoded) two-digit number. The two-digit number – generated, recorded, and stored by the computer at the time of the last transaction – serves as a password to allow access to Joe's account. After each transaction, a new number is generated and stored; a counterfeit card would not have the correct number encoded on it...
>
> Every few days Joe takes his machine-readable bills to a pay station on the corner. He calls the central computer exchange and inserts his identification card into a slot. A verification voice acknowledges him. One by one he drops in his bills, and the voice repeats instructions until the last bill has been processed."

Changes in the payment system are likely to be evolutionary in nature, and it is possible that several different practical designs for future banking systems will exist at the same time. But the underlying purpose of all the systems will be the same. The idea will be to harness the speed and massive information storage capabilities of modern electronic computers to the business of banking. (Parallel financial record systems are likely to be developed for institutions such as department stores).

The increasing use of computer systems by the banking industry could lead to difficulties for a number of reasons. First, it may become increasingly difficult to ensure the accuracy of data stored

in central computers if a large number of bank tellers and retail-store clerks can feed data directly into the computer through remote-access terminals. Inaccurate data could produce errors in an individual's financial account that might affect his credit rating. Secondly, as banking systems make greater use of telecommunication facilities, more bank personnel will have access to confidential information through computer terminals, and this would make it more difficult to prevent disclosure of confidential information.

On the other hand, the banking industry is facing competition not only within its own ranks, but from the so-called "near banks", the trust companies and the credit unions. In an industry where price competition is restricted, a high premium is placed on the quality of service. A reputation for slack security procedures or inaccurate processing is likely to affect seriously a bank's competitive position. This fact alone should provide some measure of consumer protection. Indeed it can be argued (and no doubt will be) that the greater centralization and control resulting from computerization provide an opportunity for improved accuracy and security.

This said, it should be candidly admitted that it is unlikely that the security of Canadian banks is much superior to that of the British banks where information on a man's bank balance can be bought for $15.75. Since it seems certain that the banks will continue to accumulate ever-increasing quantities of personal information, and possible that an integrated system of personal financial records will be developed, it is becoming progressively more important that information transaction procedures, both as regards the public at large and as regards organizations enjoying special privileges, should be clearly and openly stated.

2. Medical Databanks [3]

One of the most pervasive beliefs in the practice of medicine is that the doctor-patient relationship is confidential and free from third party interference. The 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, thus enabling the physician to give comprehensive medical treatment with compassion.

At least three trends may fundamentally alter this traditional relationship: the health-team approach to delivery of care, the developing health information systems, and the changing status of the health professions. The first two of these phenomena have

significant effects on the ability of the individual to protect the confidentiality of information about his health.

The health-team approach gives the patient easy access to a wide range of medical specialists and other health professionals. For the doctor it means that his time can be more efficiently used, and that he can more easily specialize in particular fields. An inevitable result of such an approach, however, is that the classical doctor-patient relationship is dispersed among a team of medical and para-medical personnel. Criticisms have been made that patient care becomes fragmented to the point of dehumanization. In an attempt to meet this criticism, some hospitals in the United States have appointed an ombudsman to represent the patients.

Health information systems are being developed with two basic objectives. The first is to provide better accounting and administrative data; the second, and more difficult, is to provide medical personnel with better information so that the patient will receive superior treatment. The two objectives are not completely separable. The provinces are currently using their medical EDP records for three purposes other than billing and accounting. These are: to control the type of medical care being delivered (patients are asked to verify charges to ensure that doctors bill only for services performed); to research into epidemic diseases and patterns of health care utilization; and to help enforce legislation. In Manitoba, the medicare records are compared with driver's licence applications to help determine eligibility for a driver's licence. It is technically feasible to correlate health records with records of other government services to ensure that legal requirements and restrictions are met. For example, health reasons are often cited in applications for welfare and other forms of social assistance.

Medical insurance records have also been used in several provinces to estimate the income of doctors. The subsequent release of some of this information to the press has led doctors themselves to complain of privacy invasion.

Several computerized multi-use information retrieval systems for health records have been implemented. Among them is the Professional and Patient Activity Studies system at the University of Michigan, which provides a record of patient treatment procedures, and to which approximately one-third of all Canadian hospitals subscribe (participation by Alberta hospitals in the system is compulsory). More recently the Hospital Medical Records Institute has been established in Ontario to provide the same kind of statistical and analytical services; about 15% of Canadian hospitals subscribe to its services.

Computer-assisted diagnosis has been introduced at a number of medical centres. Experiments in a Scottish hospital with a special computer system designed to permit the patient to provide all the basic data required for admission revealed not only that the information gathered was as accurate as that obtained from personal interviews, but also that 50% of the patients preferred the computer dialogue to dialogue with a doctor.

The Department of National Health and Welfare currently maintains health information on the disabled and blind, rehabilitation clients, native peoples in some areas, and people with communicable and chronic diseases, including tuberculosis and venereal disease cases. The Department is planning a computerized health record system for the 35,000 people in the Northwest Territories, which will give district health offices access to an Ottawa service bureau through telecommunications links. This system, which would contain information on individual health, on doctors, on facilities and social problems such as alcoholism and drug addiction, is probably the most extensive under consideration in Canada.

The centralization and computerization of medical records raise several issues often considered under the umbrella of privacy. Such concerns as the possibility of error and the use of health information by third parties, unknown to either doctor or patient, or perhaps with the knowledge of the doctor only, are obvious.

The problem begins with the input of information to the system. The many errors discovered by a life insurance company in the process of computerizing its records have already been discussed. Similar experiences have been encountered in other organizations. Unless special precautions are taken, input errors are bound to occur. But even if the transcription of data to the computer is faultlessly performed, two sources of error in medical records remain, namely incorrect diagnosis and incorrect reporting of findings.

Incorrect diagnosis occurs because a diagnosis, after all, is simply a deduction from the observed symptoms of their probable cause. The symptoms themselves are often amenable to several interpretations. In making his diagnosis, a doctor will weigh not only the possible cause of distress, but also the consequences of incorrect diagnosis. If his diagnosis is likely to be used for other than purely medical purposes, such as assessing the individual's eligibility to drive a car or to receive welfare payments, a doctor may exercise caution recording his diagnosis. This situation is accentuated in cases such as venereal disease or suspected child beating, where the doctor's concern for his own legal liability or his

patient's embarrassment may lead to deliberately incorrect reporting of findings.

Once the health record enters a multi-access databank, control over the information is often lost by both doctor and patient. Innumerable individuals may have access to and use the information without the knowledge of the subjects on record. Files can be reproduced by electronic equipment, and there is usually no attempt to account for the materials once reproduced, which may form the substance of new databanks.

The problems faced by the medical profession are brought into even sharper relief when the question of psychiatric treatment is considered. In a submission to the Task Force from the Clarke Institute of Psychiatry, the authors stated:

> "An added complication in psychiatry, as opposed to other medical specialties, is the fact that information collected on each patient stresses the family, personal, social and sexual history. It is clear that the leakage of such material would usually have a greater social impact for the individual than information on the state of a duodenal ulcer."

A problem of particular relevance to the medical profession is that of access by the patient to his own files. The Ontario Medical Association brief illustrated this problem with the following example which highlights this and other issues:

> "A physician in Ontario may wish to administer to his patient a questionnaire such as the Minnesota Personality Inventory (M.M.P.I.) This long questionnaire can then be sent to a laboratory in California where it is interpreted with the aid of a computer and a report is returned to the attending physician. The report may suggest that the patient shows definite evidence of suicidal tendencies or of schizophrenia. Many would believe that the patient should not have access to such a report. If the patient did have right of access, should he be able to see the records of the physician or of the data centre which performed the analysis? Should a data centre, in such a case, ever divulge information to anyone except the physician who forwarded the material for analysis? What would be the situation if the patient were, in fact, sane, had been erroneously labelled schizophrenic because of misinterpretation at the data centre, and then denied access to his record on the grounds that he was mentally ill?"

Many institutions permit patients to see their records only

with their doctor's prior permission and in his presence. For as long as the doctor-patient relationship is in a healthy condition, this appears to be a sensible solution. Different approaches to the practice of medicine may require different solutions.

In summary, it can no longer be assumed that it is always better to record a medical diagnosis and the treatment given than to leave such occurrences unrecorded. Before data are entered into the health records system, both the patient and the physician should clearly understand who will use the medical records and for what specific purposes.

At least some health authorities believe that privacy and confidentiality of health information will become a dead issue. It can be argued that the ability to transfer medical information freely will materially assist medical planners, practitioners, and researchers to provide society with the most efficient medical services possible. However, in order to maintain a relationship of mutual trust between doctor and patient, it is important that data concerning the patient be transferred with his knowledge and consent to the greatest possible extent. To the extent that public opinion does not support the transfer of patient records, it is important that those responsible be aware of that opinion, for it may well be that the disadvantages of the data transfer greatly outweigh the advantages. A distrustful patient is likely to withhold important information, to the detriment of all concerned.

[1] The bulk of the material on banker's data banks is drawn from the report by H.S. Gellman for the Task Force entitled *Electronic Banking Systems and Their Effects on Privacy.*

[2] Kramer, R.L. and Livingston, W.P. "Cashing in on a Checkless Society", *Harvard Business Review,* Sept/Oct 1967, p. 142.

[3] Most of the material in this segment is drawn from a report by J.I. Williams entitled "Privacy and Medical Records" which is included as Chapter 7 of John Carroll's report for the Task Force entitled *Personal Records: Procedures, Practices and Problems.*

Chapter 6
The Investigators

The function of investigation agencies is to acquire information required for certain purposes which will not or may not be voluntarily disclosed because of a mutual lack of trust between the subject of the investigation and society or some segment of society. It is therefore reasonable to assume that investigative agencies will operate according to substantially different rules from those that guide administrative and statistical collectors and users of data.

The two organizations discussed below operate under different assumptions. The activities of the police are backed by the force of law, whereas investigative credit bureaux and other private investigative bodies, such as private detectives and commercial investigators, collect information without any particular authority to do so, and must therefore rely almost exclusively on persuasion and native intelligence to gather the data they seek. While the police endeavour to enforce the laws enacted by the legislatures, the private agencies are acting, by and large, at the behest of commercial entities which are looking for actual or potential infractions of what might be called commercial or contract regulations.

The practices of data collection (as distinct from the treatment of data once collected) followed by investigative agencies have been and will no doubt continue to be a subject for public concern

and debate. Because the Task Force study was expressly limited to the impact of computers on privacy, information collection practices received only marginal attention.

1. The Police

Without doubt the most significant development in Canada in the field of police information-handling is the Canadian Police Information Centre (CPIC) scheduled to go into full operation in 1975. By that time, the Government of Canada will have spent $36 million. This Centre, which will be run in Ottawa by the RCMP, will use an IBM 360/65 computer (with back-up computer) and a large number of discs and magnetic tape units to provide access by typewriter terminal to central police files for about 250 police forces throughout Canada. Initially four files will be available (in both English and French): outstanding warrants, stolen vehicles, stolen property, and criminal records. Of these only the criminal record file, which in manual form currently contains about one million records, is of direct interest from the privacy standpoint.

Although the systems study that will determine the contents of the computerized criminal record file has not yet been completed, the likely contents of the file will include name, criminal record number, penitentiary number, fingerprint classification, charge sheet information, and criminal associates.

At present, police forces throughout Canada maintain their own comprehensive records in manual systems. It is expected that, with the implementation of the CPIC, the need for individual record systems will be greatly reduced, if not eliminated, since the police forces will have access to all criminal files in Canada. However, the controls to be placed on the use of these files have not yet been developed.

The CPIC system will rely heavily on physical security of the terminal and the exercise of normal command responsibility to provide security for the data in the system. The computer will recognize only legitimate terminals connected to the system, and an audit trail of use will be available. Encryption of data transmitted to and from remote terminals will not be employed, since the cost was judged to be too high.

It is to be expected that implementation of the CPIC will result in the publication of clear guidelines for the handling and dissemination of information about criminals, as has occurred in the development of a similar project in the United States (Project

SEARCH – System for the Electronic Analysis and Retreival of Criminal Histories).

Some current policies in the maintenance of criminal records are:

- Records are not made (and no fingerprints are taken) in the case of summary or juvenile convictions (according to provincial laws defining these categories).
- Records of pardoned criminals are kept in a separate file, with strictly restricted access as prescribed by the Criminal Records Act.
- The governing principle is whether or not fingerprints are taken. 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 a criminal dies or until he 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 police file.

It should be made quite clear that police files are far from being synonymous with criminal records. Files are undoubtedly kept on suspects who have no criminal record, and the record of an arrest which does not result in a conviction can be very damaging. Since such files will not, initially at least, be fed to the CPIC computer, it can be assumed that they will continue to be maintained locally.

It will surprise no one that information about security and intelligence files is difficult to obtain. It can be confirmed only that such files do exist, that they are not at present in machine-readable form, and that they may at some future time become computerized. Because of the extremely sensitive nature of these files, in that much of the information must inevitably be hearsay, and because of the likelihood of there being files on innocent citizens, it is, of course, of the greatest importance that disclosure of information from these files be under the strictest possible controls.

A site visit by the Task Force to the Toronto Metropolitan Police disclosed that most files maintained by that force are manual. They include: Central Index, Complaint and Victim File, Accident File, Stolen Property Description File, Stolen Car File, Summary Conviction Records and Arrest File. The Central Index contains one million cards covering individuals in the following categories: wanted persons, missing persons, criminal records,

summary convictions, suspensions, interdicted lists, probations, paroles, and juvenile contact cards.

2. Investigative Credit Bureaux

The distinction between in-file credit bureaux and investigative credit bureaux has already been made. Investigative credit reporting agencies deal primarily with individuals rather than companies. They investigate applicants for life, fire, and automobile 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 subject's employer and, in about half the cases, talk to the subject himself. Retail Credit of Canada, the largest investigative bureau in Canada, prepared reports on 400,000 job prospects in 1971.

Like in-file reporting agencies, investigative bureaux keep their files in manual form and conduct their operations on a local basis, exchanging information among branches on a national or international scale as circumstances dictate. Their investigators have no common background and turnover tends to be higher than in mercantile reporting agencies. Services are sold on a case basis ($5), or on an hourly basis ($10) for major investigations.

In a brief submitted to the Task Force, Retail Credit of Canada Inc., a wholly-owned subsidiary of the Retail Credit Company of Atlanta, Georgia, pointed out that it has a strong self-interest in maintaining accurate records, since inaccurate records lower the value of its service to its customers.

In defence of the company's investigations, the brief says:

> "Investigations which we are commissioned to make by our customers originate in an application by the person about whom we are seeking relevant information. So far no one has suggested that either life or auto insurance companies should be compelled to issue policies or rate premiums upon the basis of information which, from an underwriting point of view, is inadequate or untrue, or both."

The brief goes on to say that:

> "To give a citizen an opportunity to correct possible

> mistakes in a report, all that is necessary is to provide that the user of the report – the Company's customer – whenever the customer denies a benefit wholly or partly, on the grounds of information in a Retail Credit Report, the customer shall on request inform the subject that report information was a factor, giving him the identity and location of the reporting agency so that the subject may have an opportunity to discuss the relevant information with a senior management representative of the reporting agency."

On the question of legal compulsion to disclose sources of information, the brief states:

> "...Rètail Credit Canada believes that legal compulsion to disclose sources of information of a personal history nature would effectively dry up sources and threaten the existence of every reporting agency in this field. At the very least, the result of such a change in policy would make it difficult to develop reliable information on a subject about whom a source might have unfavourable information; unless the source was prepared to give an unqualifiedly favourable report, he would say nothing. This is turn would deny a significant number of people who are now, on balance, given another opportunity by life and auto underwriters, by granters of credit and employers, the benefit of discriminating judgment on the information now given by those who would refuse to comment."

Although many good points are made in the brief, it seems unduly optimistic to believe that those who turn down applications on the basis of credit bureau reports can be relied upon to quote their reasons for refusal unequivocally. The present system makes it easy for innocent mistakes to cause substantial personal damage.

Because of the critical importance to the individual of many of the decisions to which the investigative report contributes, an argument can be made that such agencies should be required to inform the person concerned that they are in possession of a file on him, and to give him the right to examine that file for a nominal charge. The actual source of the information is less important than the information itself. If the arguments of Retail Credit of Canada about the importance of non-disclosure of source are valid, concealment of the identity the source may perhaps be justified. It does seem important, however, for psychological reasons as much as any other, that the individual be allowed to peruse his file himself,

without the necessity of talking to someone interpreting his file for him.

Chapter 7
To S.I.N. or not to S.I.N.[1]

A much debated issue is whether or not all Canadians should have a Single Identifying Number (S.I.N.) which could be used to supplement or replace the existing identifiers of name and address, and the various identifying numbers used for such purposes as social insurance, driver's licence, bank account, and passport. Numeration is proliferating in almost all sectors of the economy despite a latent public resistance to the trend. Although no strong pressure to institute a Single Identifying Number for all Canadians is apparent, the system has been introduced in several foreign countries. Moreover, as the economies derived from the use of a Single Identifying Number become more and more apparent, it is to be expected that the pressure to institute a formal numbering system will build up. Indeed, the Canadian Standards Association is already proposing the adoption of a standard personnel identification format for computer records, which leaves room for insertion of Social Insurance Number should they be adopted as common identifiers.[2] (A similar proposal by the American National Standards Institute has led to the initiation of a public inquiry into privacy and information by the United States Department of Health, Education and Welfare.)

Pressures to introduce a single identifying number originate in

both the private and the public sectors. A survey of 250 organizations, ranging from credit card companies to hospitals, conducted by the American Bankers Association revealed that most respondents favoured the adoption of S.I.N. Indeed the United States government has recently insisted that all chartered banks record the Social Security numbers of depositors, as part of the information kept with bank accounts, in order to facilitate the retrieval of information for tax purposes. Several Canadian banks and credit bureaux have indicated an interest in S.I.N., as has the Ontario Medical Association, to which a special committee recommended that "the OMA approve the concept of a single identifying number for each individual." However, the Committee stated that as a pre-condition rights of access and dissemination and security requirements must first be resolved.

Proponents of S.I.N. claim that the citizen will derive direct benefits from the system.[3] For example, the new German S.I.N. system will permit a citizen who moves to notify his change of address to one agency, which will then notify all other agencies and departments needing this information. Although no supporting figures were encountered, it is also claimed that such efficiency of services will result in significant cost savings for the consumer.

While the proponents of S.I.N. have produced little concrete justification for their cause, neither have their adversaries produced strong evidence against it. Opposition is more visceral than intellectual, and appears to have three major sources: fear of loss of anonymity, fear of dehumanization, and fear of what might be called the cataclysm.

It has already been argued that fear of loss of anonymity is central to public concern over loss of privacy. The very reason for pressures to adopt S.I.N. – the assistance it would provide in matching files – is thus, at the same time, a primary cause of disquiet. Many people are worried that progressively comprehensive dossiers will deprive them of an essential weapon in any struggle against an organizational bureauracy – that of voluntary anonymity.

Accompanying this fear is a suspicion that bureaucrats confronted by numbers will tend to forget that they represent real people. The suspicion is fed by haunting memories of the Nazi system of numbering Jews in the 1930's and 1940's. The survey of Canadians by the Department of Communications revealed that 62% fear that computers "will reduce us to numbers".

Fear of the cataclysm is simply the concern that, should an autocratic régime come into power, single identifying numbers

would be used to assist in the compilation of investigatory dossiers which would be used as instruments of oppression. Proponents of S.I.N. point out that the lack of comprehensive dossiers has in the past had no obvious inhibiting effect on autocrats.

Identification numbers for all citizens have already been introduced in Sweden (1947), Israel (1948), Norway (1964), Finland (1965), and Denmark (1968). Preparations are under way in Argentina, the Benelux countries, the Federal Republic of Germany, Japan, Switzerland, Spain, South Korea, and East Germany.

In Denmark, there was not much opposition before the S.I.N. system was established but criticism – especially by the press – developed later, centering on the possibility that "person numbers" would make it easier to collect data on citizens and that this information might be misused. In the United States, the proposal to include the social security number in the 1970 census was dropped as a result of opposition in Congress and elsewhere.

In Canada, at present, there are no universially applicable personal indentification numbers. Use of the Social Insurance Number is mandatory only in the Canada Pension Plan, for unemployment insurance, and for income tax purposes (and, in Quebec, for the Quebec Pension Plan). The Social Insurance Number Index is maintained by the Unemployment Insurance Commission and has 13.5 million numbers on file covering almost all the labour force and a number of special groups such as school children. Plans are under way to update the file automatically to record births, marriages, deaths and other changes in the personal status of persons covered in the files. The Social Insurance Number comprises nine digits. The first digit specifies a geographic region and the last is used to check the accuracy of the preceding numbers. The other digits have no significance. In contrast, Sweden uses a 10 digit number, in which the first six digits refer to date of birth, the next three are for geographic allocation, and the last is a check digit. The Danish system also comprises 10 digits of which the first six refer to date of birth while the last four are a serial number. At the time of the establishment of Canada's Social Insurance Number, proposals to include data on date of birth and sex were rejected on the grounds these might open the door to possible discrimination by employers. The Unemployment Insurance Commission is currently considering proposals for a revision of the Social Insurance Number system; at the same time, at the request of several provinces, the number of Canadians covered by the system is increasing.

At present almost every individual in Canada can be identified

through eight or ten different types of number, e.g. social insurance, unemployment insurance, birth or citizenship registration, government medical care, government hospital care, address/apartment/postal zone, telephone, driver's licence, public utilities billing (telephone, light, heat), bank and/or trust accounts.

Additionally, most people in Canada are aware of over 20 types of number which identify them in different environments, e.g., passport, licences (boat, trailer, fishing, etc.), parking lot, high school registration, university registration, insurance policy, private medical care insurance, X-ray record, doctor's records, hospital charts, drug prescription, savings and/or other bonds, safety deposit box, brokerage account, pawnbroker, shoe repair, laundry, theatre/sports/etc. admission ticket numbers, social/athletic club membership number(s). It is not inconceivable that an "average" Canadian today could be identified through 35 or 40 different numbers.

It is interesting to note that until 1967 all Eskimos in the Yukon and Northwest Territories were identified by numbers imprinted on tags worn around the neck. Not surprisingly the Eskimos objected to the system and, in preparation for its abandonment, during the four years from 1967 to 1971 the Eskimos selected their own surnames which are now used in lieu of numbers. Neither the old disc-number files nor the new registry of names contains data other than that normally recorded at birth.

Computer filing systems work much better if every record carries a code number; names and addresses are unreliable indicators when the matching of different records depends entirely on computer logic. While human intelligence will make the reasonable assumption that a Mr. A. Brown of 12 Thorncliffe Park Drive in one file is almost certainly the same person who appears elsewhere as Mr. A.G. Bown of 12 Thornclyffe Avenue, the computer much prefers to know him as 418-851-218.

Code numbers also help to avoid duplication where different people have identical names. In addition, the exchange of data among computer systems is less expensive with code numbers because the number of digits in the identification number is far less than the number of digits and letters in the name and address. Thus, less space is needed inside the computer to store the identification number and less time taken to sort the file.

The use of personal identification numbers can make record linkage easier but does not solve all the problems of file integration. For example, even if two sets of computer files were linked through the use of a personal identification number, in many cases the file

formats are not compatible and the information could not be retrieved automatically without human intervention. To make two separate computer files compatible usually involves a considerable amount of time and money for translation and conversion. On the other hand, if Single Identifying Numbers were adopted in Canada, it is likely that system designers would tend to place more emphasis on file compatibility so that, in the future, computer files could be linked more easily. The standard proposed by the Canadian Standards Association for identification of individuals for direct machine information interchange represents a significant step in this direction.

Some provincial government agencies have been reluctant to adopt the Social Insurance Number for their files. For example, the Ontario Department of Transportation and Communications did not adopt the Social Insurance Number for driver's licences because it does not contain enough intrinsic information. Instead, Ontario adopted its own driver's licence number system, which contains some information about the driver, such as the date of birth.

Two major new income security programs will, if introduced, extend the use of the Social Insurance Number. The Family Income Security Plan (FISP) will, since the cheques will be payable to mothers, require the registation of those mothers wishing to benefit. Proposed Old Age Security legislation will also require the use of a Social Insurance Number. The scale of benefits from both programs will be income-related, and it is expected that stated income will be confirmed by the Department of National Revenue.

It is possible that a *de facto* personal identification number will develop in Canada, either through an ever-widening use of the Social Insurance Number (despite its limitations) or indirectly through credit card and bank account numbers.[4] However, it is important to ensure that a Single Identifying Number should not be adopted in Canada, directly or indirectly, without a full examination and public debate of its merits and consequences.

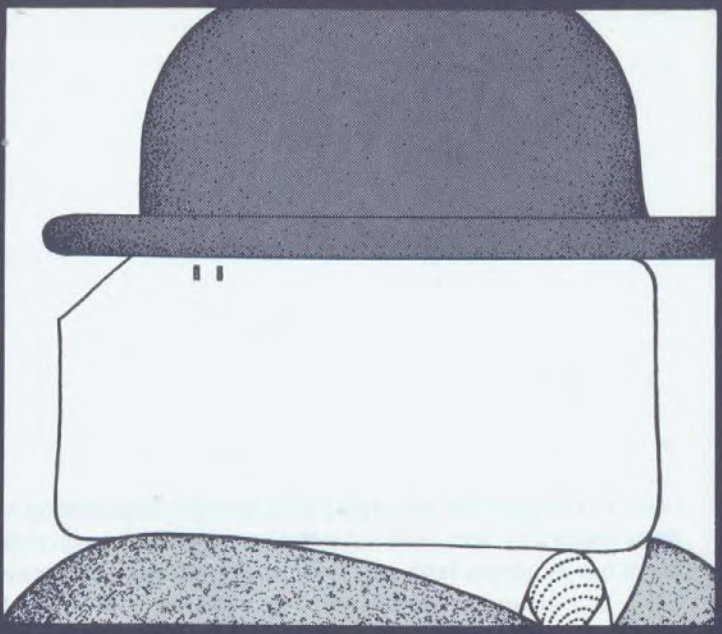
[1] The material in this chapter is largely drawn from studies for the Task Force undertaken by H.S. Gellman and C. Kirsh entitled *Statistical Data Banks and Their Effects on Privacy* and *Profile of Personally Identifiable Records in Canada* respectively.

[2] Draft CSA Standard Z243.9, "Identification of individuals for Machine to Machine Information Interchange", 6th draft, Feb. 11, 1962, 11pp.

[3] *PERSONNENKENNZEICNEN*, a booklet published (in German) by the Federal Department of the Interior, Bonn, Federal Republic of Germany to explain the proposed German personal numbering system. June 1971.

[4] U.S. chartered banks are required by law to identify all individual accounts by Social Security Numbers to permit identification in the event of tax fraud investigations.

Section III



The Impact of Computer Technology

Chapter 8
The Technological Prospects[1]

The present and following chapters deal with aspects of computer technology relevant to privacy. This one examines some developing technological trends, while the next examines the much debated question of security in a computer environment.

As has already been observed, the computer by itself neither can nor does invade privacy. But it does make more frequent the occasions when this might happen: by permitting the storage and rapid retrieval of vast quantities of data; by encouraging the rapid dissemination of that data over any distances; by facilitating the centralization of data and by making possible the compilation and analysis of extensive tables of statistical information. Although the technology is far from being fully developed computers can already sort and merge large data files to derive individual dossiers based on disparate information.

Computers also have facilitated, and even encouraged, a human tendency to equate information with wisdom, and hence a tendency by some people to collect information for its own sake. To the extent that decision makers come to depend upon information provided by computuized systems, so they may magnify the

importance of that data which is quantifiable. The Harvard University *Program on Technology and Society,* in its final, 1972, report, commented:

> "The results of computer simulations and systems analyses are delivered mainly in a quantitative form which can lend an aura of rigour and infallibility not justified by the hardness of the data or the validity of the assumptions on which they are based."

The capability of computers to sift through large quantities of data and to associate seemingly unconnected events has been somewhat oversold in terms of today's technology. It is not uncommon for large files to require over 100 reels of magnetic tape for storage. Since it takes several minutes for a single tape to be read just once, it is clear that complex searches of large files are both lengthy and costly. Indeed, many searches that have been envisaged would require extensive (and expensive) reprogramming. Technological developments are, however, swiftly reducing the cost and difficulty of such searches.

It is clear, nonetheless, that computers can be exploited to protect privacy. Automated systems can be readily programmed to maintain an audit log of the uses made of a file; and it is a relatively simple matter to provide computer printouts of files if a subject wishes (and is allowed) to examine them. Furthermore, the very fact that computerization often leads to centralization of files means that file accuracy is easier to maintain, and that privacy controls can be more easily exercised.

1. The State of the Art

A parallel can be drawn between the state of the automobile industry in the early 1920's and that of the computer industry today. The primary impacts of the automobile (e.g., more highways, enlarged steel industry) were predictable; the secondary and more significant impacts (e.g., the growth of cities and the megalopolis, pollution) were by and large not foreseen, at least not by those who could take appropriate action.

With the computer today, it is commonplace to say that the surface of the applications of computer technology have hardly as yet been scratched. In this chapter some attempt will be made to examine what might be called the primary effects of computers; the long-term impact unfortunately can only be a matter for speculation. For example, Engelbart[2] at the Stanford Research Institute is working on what he calls "augmenting human intellect". His work,

which is receiving substantial support from United States research agencies, is aimed at building a new working environment in which the emphasis is on how people work together. In this process the computer is but a tool, albeit an essential one, which helps the individual to collate relevant information, to view it from different perspectives, and to converse through the computer with other workers.

The impact of Engelbart's work is difficult to foresee, but in the nearer future there are developments with potential impact on privacy which are easier to predict.[3] It seems likely, for example, that within the next 10 or 20 years most recorded information will be in computer-readable form. The principal impediments to this trend are the high cost of random-access storage devices and converting material into machine-readable form. However, the cost of random-access memories is decreasing quickly, and the introduction of computer-typesetting techniques and computerized text-editing facilities (such as that used to produce this report) means that much original material will be in digital form in the first instance, and will thus require no conversion. Furthermore, the use of optical scanning techniques has done much to reduce the cost of converting printed material to machine-readable form.

The computer has been developed at an extraordinary pace. The first successful digital computer was produced in Germany in 1941. Two early landmarks were the Harvard Mark I computer of 1944, which required 4.5 seconds to perform a multiplication using electromechanical relays, and the first all-electronic computer, ENIAC, which became operational in 1946 and was about 2,000 times faster than the Mark I. In contrast, the fastest computer available today is capable of operating approximately 500 million times faster than the Mark I. Since 1952, when computers started to become generally available on a commercial basis, the average cost for execution of a single instruction has been reduced by a factor of about 1/10,000.

Although computer speeds and costs will continue to improve, some slackening in the rate of advance is to be expected. New technologies now in the laboratory (such as optical processing, Josephson effect devices, associative processing) show promise of increasing processing speeds 10-fold over the decade, while the widespread use of integrated circuits for logic and for rapid-access memory could result in price reductions of up to 1/100 in the same period. However, the existence of these potential capabilities does not in itself dictate the timing of their arrival in the market-place, which will also be affected by economic and social considerations.

Up to the present, the major computer manufacturers have been able to price their equipment in the neighbourhood of 10 times their manufacturing costs. This high mark-up has enabled a high growth rate to be maintained, since capital was readily available for expansion, for research, and for concentrated marketing. It is debatable whether such a high ratio of selling price to manufacturing cost will be maintainable over the next decade. Provided that the computer equipment market remains competitive, it seems inevitable that profit margins will decrease as the technology becomes more widely understood.

Worldwide investment in hardware, software, and manpower development now exceeds $100 billion. In Canada, the investment in computer-system equipment alone exceeds $1 billion. The annual growth rate of investment in computer equipment, in both Canada and the United States, has been in the range of 17 to 20%, averaged over the past five years. By 1980 Canadian investment in computer equipment is likely to be well in excess of $4 billion.

Much of the impetus behind the rapid technological developments has been provided by massive support from the United States government, primarily through the Atomic Energy Commission and the Department of National Defense. It appears likely that, during the 1970s, business and citizen-oriented government projects will provide the spurs for technological development.

The largest technological cause of cost reduction appears likely to result from savings in storage costs. Within the next few years large institutions are likely to acquire on-line memory systems containing 10^{12} or more bits (compared to capacities of 10^9 bits today) and to achieve reductions in storage costs by a factor of 1/100 or more. Since memory capacity lies at the heart of information processing systems, improvements in this area will have a significant impact on the nature and operational power of databanks.

Drastically decreasing costs of electronic circuitry have permitted a lot of heretofore "large computer sophistication" to be built into minicomputers. Such features as Fortran compilers, and hardware multiplication and time sharing software are no longer unusual on minicomputers. This new found versatility of minicomputers is complemented by the substantial economies of scale achieved by super-computers, particularly in computer-intensive applications and those requiring extensive manipulations of large files. An important factor is the development of very large data-storage systems, which require large capital outlays but have very low costs per unit of data recorded. For relatively fast-access

memory, increasingly large discs and drums will become available. For slower-access bulk storage, high density tape-transport systems and laser and holographic memories show promise of reducing storage costs from approximately .01 cents per bit for current tape systems to somewhere in the order of .00001 cents per bit by the mid 1970s.

Super computers require high utilization to make them economic; thus for many applications, they must be able to receive remote-input data at reasonable cost. Computer communications traffic already accounts for about six per cent of total telecommunications revenue in Canada, and is growing at about twice the rate of voice traffic. Distance-dependence of digital transmission rates will be substantially reduced as long-haul transmission facilities consume an ever-decreasing proportion of the communications dollar. Although tariff bases will undoubtedly change, making direct comparison difficult, it seems likely that by the end of the decade long-distance data-transmission rates will have been reduced to between one-third and one-ninth of their present levels. As costs of long-distance digital transmission decline and standards of service improve, centralization of computerized data bases will become increasingly economic.

Towards the end of the decade, pressures will develop for a number of computer-associated services in the home, although they are most unlikely to become generally established during the 1970s. Initial services to the home are likely to make use of Touch Tone telephone sets with voice response from the computer. Some rudimentary systems of this nature are already in operation.

The further development of time-sharing techniques, coupled with cheaper digital telecommunications and terminals, may do much to counteract the centralization of power which appears to follow on the centralization of information systems. For, while economies of scale may well lead to centralization of information storage, technologies associated with time sharing and digital telecommunications permit highly decentralized access to the information. Power conflicts based on rights of access are therefore likely to become increasingly common as centralized data sources of greater potential come into being. The recent confrontations over access to university libraries may be only the first skirmishes of a new struggle for information.

A popular current pastime in the technological journals is to suggest that the development of computer hardware technology has greatly outstripped software or programming technology. The disappointing performance of many highly touted and expensive

management information systems (M.I.S.) is often cited as evidence of this. A slogan that embodies a more accurate diagnosis of the problem labels the 1970s as the "decade of the [computer] user".

The early development of the computer industry saw relatively sophisticated manufacturers selling equipment to bedazzled but, by and large, uncomprehending customers. The greatest success accrued to the manufacturer who offered a complete service, thus unburdening the customer of many decisions he felt incompetent to make. It is small wonder that in those circumstances there was a surfeit of systems that failed to meet either implementation and cost schedules or design specifications. Even relatively simple systems for which the design parameters were known (such as payroll systems) encountered problems. Management information systems, which purported to provide middle and upper management with necessary information, had a slim chance of success in such an environment. The most urgent need was more systems analysts who understood user problems, and, perhaps more important, for more potential users who understood the capabilities and shortcomings of computers. Not surprisingly, this convergence of understanding is happening rapidly, with the result that the user is winning back control from the computer manufacturer.

In an article published in 1970, a consultant from A.D. Little Inc.[4] stated that it was his conclusion and that of his associates that "no important new software functions are likely to be developed between now and 1975, and none are needed." He went on to say, however, that there are serious problems in making known functions work properly. Certainly there will be incremental improvements in computer languages, and much better data-base management systems will appear. Many new and useful applications systems (using existing software technology) will also make their presence felt. In addition, the rising proportion of the computing dollar spent on software (as hardware costs decrease) is likely to shift developments away from efficient use of the hardware towards the more efficient use of the programmer and analyst. But, apart from these trends, the principal forecast for technological development in software is the use of the computer itself to assist in program design. Work in this area could conceivably have an enormous impact on the economics of computer program development in the latter part of the decade.

2. Summary of Trends

On the basis of the foregoing discussion, some general conclusions about computer technology trends can be made.

1. Further reductions in the cost of computing equipment will make viable many applications that are now uneconomical or only marginally economical, such as on-line banking and credit, and new medical and educational systems.
2. Ultra-high-speed computers, coupled with very large on-line memory systems and sophisticated data-management software, will make it economically possible to search large and disparate databanks for the assembly of information in new categories, a capability that will be heavily used by governments and business to develop simulation models of possible courses of action. This development will increase the need for detailed, accurate information of all types, including personal data about individuals.
3. Enormous economies of scale are now possible in the manipulation of large databanks. The relatively high capital cost of large memories will also be a strong incentive to economize by centralization of digital data files. This need not necessarily entail, for example, the concentration of all files on a citizen into one large digital dossier containing medical, criminal, taxation, and employment information; but it does mean that such files may well be located in the same room and hence make data interchange more convenient.
4. A very large percentage of medium and large computing systems will be connected to remote locations by telecommunications facilities. The extent to which this capability is used to centralize or decentralize information will have important repercussions on political structures as well as on informational privacy.

Thus far the effects of computers upon people and their affairs has been mixed. While their beneficial effects are clear enough, inaccuracies have abounded, depersonalization has been encouraged, and power has been further centralized. In the early days of computers few people were sensitive to its potential human effects or had enough familiarity with the computer as a tool to make it

behave as desired without unwanted side effects. The necessary knowledge and sensitivity are growing, and provided the will is present the computer can provide a tool for dispersal of information and power, and for the maintenance of privacy and individuality in an increasingly complex society. It can do this by catering to all individual needs in a way which only the wealthy and powerful can now afford. Insensitive or wilful use of the computer could, on the other hand, lead us closer to a 1984 society.

[1] The material in this chapter is drawn from a report prepared jointly for the Privacy and Computers Task Force and the Canadian Computer/Communications Task Force entitled *Technological Review of Computer/ Communications.*

[2] See, for example, Lindgren, Nilo, "Toward the Decentralized Intellectual Workshop", *Innovation No. 24*, Sept. 1971, pp. 50-60.

[3] See, for example, Niblett, G.B.F. *Digital Information the Privacy Problem*, O.E.C.D. Report SP(71)4, Paris, March 1971, 42 pp, p. 4-8.

[4] Withington, Frederick G., "Trends in MIS Technology" *Datamation, Vol. 16*, No. 2, February 1970, p. 108.

Chapter 9
Security in Computerized Databanks[1]

If the dissemination of personal information stored in computer databanks is to be controlled, then a secure environment must be provided for the storage and treatment of data. The whole subject of computer security has been widely discussed during the last few years, not so much in the context of individual privacy as in the context of industrial security, where computer owners are vulnerable to revolutionary or employee sabotage and industrial espionage. Governments, and particularly the military, have long been faced with the problem of protecting confidential data in a computer environment.

There is some colourful folklore surrounding computer security. It is probably not true (as often rumoured) that a programmer for a large bank instructed the computer to assign all fractions of pennies rounded off financial statements to a special account (his own) and so became rich. It is technically true that a saboteur with a small pocket magnet can ruin magnetic tapes containing valuable data; however the time required to destroy data in this way makes it unlikely that he could successfully erase more than a hundred tapes or so in an evening's work. It is certainly true that an

employee of a bidder for a large software and computing contract, through knowledge of the correct passwords, was able to "steal" a proprietary program from the computer of the principal competitor simply by dialing up the computer and asking the right questions. The thief was detected only because it happened that the program was simultaneously printed out in the main computer room, and someone idly wondered who would want to use that program at that particular time.

Ultimately, the security of data depends on some combination of controls. No such combination is completely secure; the degree of security is really a function of the cost to the intruder of bypassing the combination of locks in relation to the value to him of obtaining data in this way. In turn, for someone wishing to maintain the security of data, the cost of devising and implementing the controls must be small in relation to the cost of a breach of security. As stated in the brief submitted by the Telephone Association of Canada:

> "Neither communications networks nor computer and databank systems can ever be fully secure. Regardless of how good the encrypting or protection technology that might be applied, security measures can be broken if the pay-off warrants the trouble."

In the case of military intelligence databanks, the information they contain is considered to be of such value that almost no cost is spared to ensure data security. Such systems, however, are clearly exceptional, and this chapter deals instead with commercial or public databanks where expenditures on security have thus far been on a much more modest scale.

There are two extreme attitudes to security of data in automated systems. One approach, usually taken in a highly-sensitive installation, is to guard the entire computer system, to permit only persons with security clearance near the hardware, and to use encryption whenever transmission of data is required outside the secured area. The other extreme is found in a time-shared computer with many remote terminals (often available on a telephone dial-up basis), where the access rights to files may be assigned by one user to another, and where security measures such as password protection are available but not mandatory. Both these extremes evade the problem of protection in a system containing both sensitive and non-sensitive data.

Since the advent of large time-sharing computers, it has become increasingly desirable to allow a mix of jobs with varying

security requirements to run on the same computer. In these circumstances, it is important to be able to provide reasonable security without isolating the computer from remote terminals and forbidding the sharing of data or programs among users.

The old saying that a chain is as strong as its weakest link is often mentioned in discussions of security measures. Provision of a secure environment inevitably involves a package of measures, since protection on only one flank is little better than no protection at all. In particular, the physical security of the installation and the steps taken to ensure that personnel are honest and loyal are at least as important as some of the sophisticated protection measures which can be provided within the computer system itself.

Some of the more important aspects of a secure computer system are:

1. Protection by Password

Passwords most commonly are used in interactive (time sharing) computer systems, and are a useful deterrent to snoopers. Passwords must be stored in two places, i.e., with the user and with the system. In each place they can be subject to unauthorized disclosure. A system of one-time passwords, whereby each time the system requests the password from the user the next word on a predefined list is offered, has been suggested to counter the objection that passwords may be intercepted during transmission. Intercepting one password does not then provide the intruder with continuing entry capability. The use of one-time passwords in computer systems is rare, however, because most potential users claim it would be too much bother to keep track of the list.

Almost all computer systems require a user to have an authorization (account) number to which charges can be assigned. This number is inadequate for all but the most lax of security environments, since it is frequently printed out for accounting purposes and for identification of computer output. Furthermore it is awkward to change an account number if it is being misused. Passwords should be changeable as often as desired by the user.

Passwords can serve as authentication of a user's identity to permit access to the computer system, or can be used to authenticate the authorization of a user to access a particular file. The password for a file might be stored in the table of access rights alongside the user's account number or it might be part of the label stored with the file. The password on a file serves as a second line of defence against impersonation.

2. Protection by Encryption

Wiretapping or electromagnetic eavesdropping is a security threat whenever information travels over wires that are not in a secure area. Many systems use common carrier facilities, and here the problems are well known. Sensitive data to be transmitted from one location to another should be transformed, i.e., encrypted, to ensure privacy. The best encryption techniques involve data transformation keys that are as long as the data to be encrypted. The string of characters for the key is generated from a basic starting number as a sequence of pseudo-random numbers. The same starting value yields the same sequence every time. It is nearly impossible to determine the starting value and the generating algorithm from eavesdropping on the transmission.

Breaking a code of this type entails an enormous amount of work. For example, there are 10^{26} usable substitutions of the 26 characters of the English alphabet. The adequacy of the particular code as a deterrent depends on the degree of penetration that could be attained if the code were known. If a system uses many keys and they are frequently changed, then even a few hours per key may be more than the penetrator's resources could afford.

Devices now exist, and have been used for a long time for diplomatic messages, for transforming a string of characters into another (encoded) string, where the key to the transformation is generated by a device which is set up on buttons or wheels. The device is really a special-purpose computer, and its operation could be programmed on a minicomputer if desired. The minicomputer would then have to be kept secure and under the supervision of a system security officer. The computer function at the central transmission terminal could be done by the main computer itself, so that separate computers would be required only at the remote stations. Several devices which will encrypt and (at the receiving end) decode data are now commercially available.

It is possible to arrange such devices to encode the input string or not according to special control characters in the string itself. For instance, in a personal file the identifying fields might be encrypted, the numerical fields not. Statistical data-processing operations could then be done on the file without decoding, while the information relating the numerical values to people would be unreadable unless the code were known.

3. Limited-access Control

Not only is it often desired to limit access to a particular file to a single individual or to a small group, but it may also be desired to limit the access by some individuals to only certain portions of the data. For example, in a hospital patient-file it may be desired to limit the access of X-ray technicians to the records of designated patients only. The accounting office, on the other hand, may need access to the records of all patients, but may be prohibited from examining the files that contain the medical diagnosis of illness. A researcher might require access to all fields except those containing the patient's name and address.

Most often, persons having access to a file have access to *all* fields of *all* records. In a manual file in which records are maintained in documentary form, it is difficult to arrange things otherwise. In a computerized system, however, right of access can be controlled either to specified records (for example, the files of certain individuals only), or to particular fields (e.g., billing information only), or to combinations of the two. File alteration privileges, if given, can be similarly specified and, in addition, alterations can be restricted to any combination of the three operations of deletion, addition, or alteration of existing data.

The access rights of a user must be explicitly denoted in any situation where partial rights exist, e.g., for a limited-access file, or where reading is permitted but changes and deletions are not. It is possible to have a table stored with the data (or separately) showing a list of authorized users of the data and their access rights. Access to this table must be strictly limited to persons authorized to modify the table, usually only the owner of the data himself.

In many cases, access control is assigned to the computer software system (or monitor) itself, since in most computer systems operations pertaining to the read or write functions are already under central control. Data protection can be provided at several levels within the operating system. Because of the enormous complexity of modern computer operating systems, it is difficult to avoid entirely the occurrence of some chance "trap doors" that permit unauthorized data tranfers between users.

4. Audit Logs

All computer systems have accounting programs that keep a log of all events significant to charging for computer services. These logs do not always record events that have no charge-generation function. Since security cannot be absolute even though operating systems have improved enormously, audit trails are essential to the detection of security violations. A straight log is often very difficult and time-consuming to interpret; rather the analysis should be done by the computer system itself. If the analysis of suspicious events, such as incorrect passwords or attempts to read beyond the assigned range of core addresses, is done as the events take place, an alarm can be set off. There are various levels of severity of action on alarm, which range from expelling a user or shutting down a transmission line to locking all files. The audit log can be sorted to reveal any particular kind of peculiarity and should be a standard tool available to a system security officer.

The operating system should be fully documented and available to independent program audit teams to ensure that necessary controls are maintained and have not been short-circuited in any way. Finally, it must be remembered that if access to the operating system itself is not strictly reserved to the system security officers, the audit and the alarm system may be turned off by an intruder.

5. Physical Security

The fashion of having computers prominently displayed to the public is dying out. The need for precise environmental control has always meant that hardware was housed in special rooms, but it is increasingly apparent that protection and control of access to the rooms is critical to security. Not only could the equipment be destroyed but data could be viewed by strangers while being printed or displayed. All persons having access to the rooms where hardware is kept should be properly identified and have a genuine need to be present. Systems of identification badges are common. Sometimes access is controlled by a security officer, sometimes by locks opened by badges or by combinations. Many installations require visitors as well as regular staff to wear authorization badges when in a computer centre. Unfortunately many of these badge systems are unenforced and provide only a semblance of security.

Where a piece of hardware is attached to the main computer hardware through a remote connection, the terminal equipment is

often under minimal or no surveillance. For this reason, highly sensitive data are rarely handled in a computer system with remote terminals. It is important that remote users and the terminals used be properly identified, not only at the time of beginning a "conversation" but from time to time during an extended interaction. This is rarely the case except in defence systems. Remote terminals provide an infiltrator with some of the largest loop-holes in a system.

The destruction of obsolete data is standard for hard copy but is often neglected with data on tapes or in core store. Since the recording operation pre-erases the previous recording, it is customary to leave tapes and core with whatever information was last recorded on them. Sensitive data should be erased by the user by writing meaningless strings of characters into core store. Tapes and discs are more difficult to erase and may require several writings of hash to remove residual information. Some security experts maintain that data can never be completely erased from magnetic tapes or discs, no matter how many times characters are overwritten. In a normal environment, however, tape destruction, as required for full military security, seems unnecessary.

6. Personnel Security

Anyone entrusted with access rights to data is a potential security leak for that data. The most direct method of access for an intruder is often through a person in a position of trust. This problem is well known, and several methods are used to decrease the probability of a betrayal of trust. Amongst these are personnel investigation to determine trustworthiness, and the imposition of penalties for breach of security. Above all, the opportunity for accidental disclosure should be minimized by having precise security procedures with regard to labelling of sensitive data, locking of file cabinets, etc. The problems here are identical with those of security of data in a manual system.

7. Current Practices and Cost Estimates

Few of today's computer software systems have provided more than the most elementary security facilities. To a large extent this reflects the current lack of demand for such protection. Virtually all high-security systems work in an isolated, shielded, and

protected area, and treat all data as confidential. In such circumstances, there is no real need for sophisticated software checks.

Responses to the questionnaire revealed a surprisingly high interest in security measures. Of the 475 responses to the question on security (only those with computers were eligible to reply), 72% exercised some kind of control over physical access; 38% used some kind of hardware/software security measures such as passwords or encoding of messages; 42% had instituted special checks on the integrity of their staff; 57% used audit logs or some other monitoring method; and 68% had procedures and rules for data disposal.

Recently, greater effort has been devoted to the provision of security in a time sharing-environment. Task Force personnel had the opportunity to examine the security procedures at one commercial computer-service bureau. These organizations are atypical in that they have a much higher than average incentive to provide a secure data-processing environment (since their continued existence depends in large measures on keeping client information confidential). However, the security practices of the bureau examined provide a useful insight into the sort of commercially practicable security procedures now available. Security provisions were as follows:

Physical security – All employees wear badges that are plainly visible. Access doors to the computing area have 10-button combination locks, and at least four operators are on duty at any time. The senior operator controls entry to the computer room and ensures that the entry log is maintained. Operator interventions with system operation (such as the mounting of computer tapes) are recorded automatically by the system.

Organizational security – There is a Data Security Officer and an alternate, both of whom report to the manager of systems. The Data Security Officer issues passwords and supervises the programming of special security routines on the computer. All computer personnel have industrial security clearances processed by the federal Department of Supply and Services.

Files – Job control cards are analyzed for tape or disc pack requests. A computer-based index program checks the serial number of the tape against the owner's account numbers, and types its output on consoles in the tape library. If the owner's and requester's account numbers do not match, a manual card file is consulted for the owner's written authorization for the requester to use the file or for user-defined security instructions. A library file extraction log is maintained.

Teleprocessing – Sign-on is by password. These passwords are

changed by adminstrative procedure. There are no terminal identification checks on low-speed circuits. The low-speed sign-in procedure requires the user to transmit his account number, user identificaton, and password. Access is restricted to files labelled with the user's identification. A log is maintained of terminal access (sign-on/off).

Encryption – Data coming in from remotely entered jobs is scrambled by a simple 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.

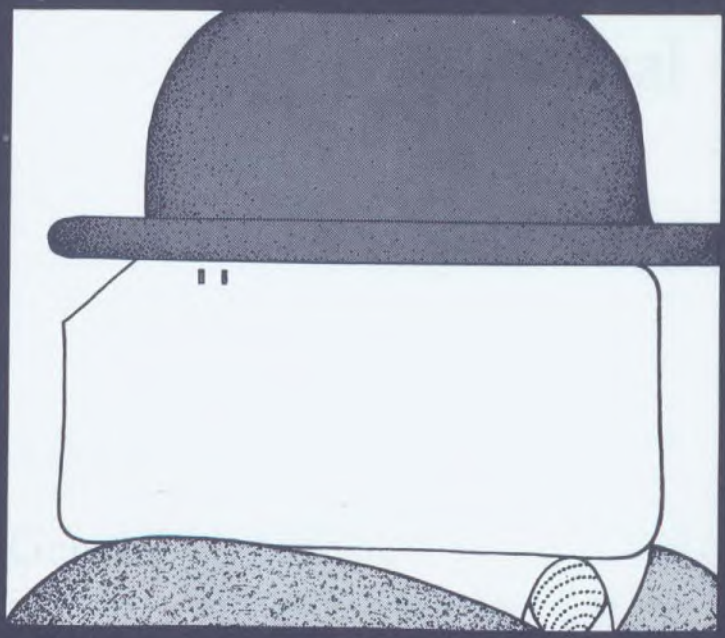
The procedures described by no means represent the ultimate in security procedures. The company interviewed rather believed that they represented a reasonable trade-off in today's environment between the customer's demand for security and the price he was willing to pay for it.

Various estimates of the cost of providing reasonable data security in a time-sharing or remote-batch environment have been made. In a study carried out by the Task Force, it was found that good protection could be provided at a cost of about three per cent in data storage requirements and twelve per cent in central processor run time. This system included such features as the separation of data header information from the data itself, the erasure of used data, the encryption of data and a test to ensure that data had not been altered without authorization. It did not provide protection for data at the level of a field within a record. The 12% cost estimate is generally in line with a number of others which have been published. The optimistic forecasts of the extra costs of security provisions are about five per cent, while the pessimists tend to estimate closer to fifteen per cent. IBM recently announced that they planned to invest $40 million in the next few years in the development of security protective hardware and software for their computer systems.

Provision of security is ultimately the responsibility of the organization handling the data, although, as an official of Senator Ervin's Sub-committee on Constitutional Rights in the United States suggested to some Task Force members, there is a useful parallel to the automobile industry in that the computer equipment manufacturers have a responsibility to provide the "safety belts and brakes" (i.e., the necessary facilities for provision of reasonable security) on their systems, and to educate customers in their use.

[1] The information in this chapter is drawn almost exclusively from a report to the Task Force submitted by C.C. Gotlieb and J.N.P. Hume entitled *Systems Capacity for Data Security*.

Section IV



The Specific Areas of Concern

Chapter 10
The Information Process and the Individual

1. General

The picture developed in the preceding chapters of the flows of personal data about Canadians, and of the systems in which these data are stored, helps to illuminate some of the issues that lie beneath the surface of the complex relationship between personal privacy and information. What is clear is that many of the issues raised bear directly on privacy and related interests and values. It is equally clear, however, that some of the issues do not relate to privacy at all but rather to the political power that derives from the possession of information.

While one can agree with the Ontario Medical Association that "people, not computers, invade privacy," the critical fact is that computers shape, and to a degree even predetermine, the ways by which people may invade privacy. Computers, as a consequence of their own efficiency, break down many of the protective barriers of inefficiency which in the past helped to shelter privacy. Computers make it far easier to merge separate files about the same

individual into comprehensive dossiers. They make it possible and relatively inexpensive for almost limitless quantities of data to be dispatched almost anywhere, particularly when electronic communications facilities are used. These striking capabilities in turn give rise to fears – some fairly extreme – that computers may lead to human manipulation, may obliterate privacy, or may reduce people to numbers. Of the people surveyed by the Department of Communications, 62% agreed with the proposition that "computers make you think that individuals are just becoming numbers." The pressures already evident in various administrative and political quarters in Canada for the creation of a S.I.N. (Single Identifying Number) system are no doubt contributing to this unease.

While the Task Force investigations indicate that much of the most personally sensitive data in Canada has yet to be automated, many of the threats to privacy and related values that automation heightens and exacerbates are already present in all types of large information systems. Information stored in a manila folder, or scribbled for that matter on the back of an envelope, can cause as much harm if misused as the most impressive computer printout.

It is therefore timely to examine the problems raised by information systems in general, when automation, which is rapidly proceeding, has triggered social concern about the problems but has not yet carried them beyond manageable proportions. Although 53% of the people surveyed by the Department of Communications believed that "Computers will cause violation of confidentiality," and although awareness of and participation in the computers-and-privacy debate is increasing (particularly at the governmental level) in many countries, the Task Force did not conclude that the problems have yet reached crisis proportions. It nevertheless recognized that this situation could change quickly and took note of the argument of some observers that, as with other social problems, there is always the possibility of a large part of the public becoming conditioned into indifference.

It appears that the institutional character of databanks (public or private) has little effect in determining the extent to which they may pose problems for people. Instead the critical factor is the nature of the information itself: the operational procedures of, say, police and investigative reporting agencies tend to be similar because both are handling similar types of information.

Among the classes of people about whom information is most likely to be gathered and processed, it appears that those in search of jobs, housing, credit, or welfare are most susceptible, since in

order to obtain benefits they must disclose large amounts of personal information. The case of welfare schemes is particularly important, since it involves the extensive computerization of information about increasing numbers of people who are highly dependent. The more effectively information is gathered and used, the more effective the welfare schemes may be, but the more extensive the erosion of privacy may also become.

The Task Force did not search out specific instances of invasions of privacy because it lacked the capacity to assess such allegations. However, enough was learned to provide a guide to the occasions when privacy is most likely to be threatened.

2. Data Gathering

A detailed examination of data-gathering practices and procedures was not central to the terms of reference of the Task Force. Nevertheless data gathering relates directly to privacy insofar as it involves the extraction of information about individuals from them or from their neighbours, employers or friends. What the Task Force did learn in the course of its inquiries was that most databanks are operated without the benefit of clear guidelines that designate what type of information should be collected in order to fulfil the approved objectives of the databank. There are few safeguards, for example, to counter the tendency of private corporations and particularly government institutions to gather more information than may be necessary for the purpose at hand; or to control the collection of information that might subsequently provide the basis for racial, religious, or other unjust discrimination. Nor are there, except occasionally, limitations on or rules governing whom data might be collected from, despite the expressed public concern about the practice of some investigators who make unauthorized inquiries among the friends and neighbours of a subject, a technique that renders the final dossier vulnerable to hearsay, and to gossip which may be founded in prejudice and malice.

The Task Force also found that those who actually collect information are often among the lowest-paid, least-trained members of their particular organization. In addition – and certain institutions such as Statistics Canada are notable exceptions – those who collect data are often sent into the field or into people's houses with only the most loosely worded guidelines on how to conduct themselves, particularly in respect of preserving the confidentiality of the data they gather.

3. The Contents of Individual Files

At least four attributes of information on file about an individual can raise difficulties for him: where this information is derogatory, harmful, inaccurate or irrelevant. There are few general guidelines relating to these questions, or generally to the contents of files.

Although few institutions set out to collect derogatory information as an end in itself (investigative and intelligence agencies are obvious exceptions) such information does get collected and filed. As yet there appears to be no bar to derogatory information being collected and handled in the same manner as any other information. While the law of defamation is well-developed, it does not in general prevent derogatory information from being collected and even disseminated provided the information is true.

Harmful information differs from derogatory information in that it can cause damage only in the context of particular uses of the information. Thus, knowledge of an individual's age, which is not a piece of derogatory information on the face of it, could prevent him or her from getting certain jobs. Like derogatory information, however, harmful information, although not strictly speaking a problem of privacy, is obviously closely related to it in that both evils are often present in the same action, such as where information about a person's drinking habits is passed on to an individual's bank manager, without his or her knowledge.

Whether or not inaccurate information is harmful, it can lead to problems for individuals. It has been shown that databanks contain more inaccuracies than is generally recognized or admitted. The exchange of information between databanks, a growing practice, may result in a single item of inaccurate information causing harm to an individual on different occasions and in different contexts. Here, a variety of values and interests – including privacy – will be served by the development of techniques and procedures for correcting files and generally rendering them accurate.

Finally, on the question of the relevance of information on file, including obsolete and unncessarily detailed information, again guidelines would be helpful. These could pertain to the types of data that are relevant for particular purposes as well as to the disposal of inactive files, for example criminal history or past

payment defaults, so that an individual's past does not haunt him forever.

4. Data Storage and Handling

The Task Force learned that while many databanks have programmed security standards and procedures to guard against "leakages" of information, and to ensure that only authorized personnel gain access to particular files, others had given very little thought to the problem. Indeed, among many of those that had adopted security measures, the protection of privacy had not been one of the primary reasons. In any case, there appeared to be some sensitivity to the problem of data security.

The effectiveness of technical security standards highlights a point that is often overlooked: the very efficiency of computers, troubling when viewed from one perspective, can be turned around to protect privacy. Strict security standards can be enforced more easily in automated than in manual information systems. Moreover, an audit log can be kept of all the uses made of a file, and it is a simple matter to provide computerized printouts of particular files if a subject wishes to examine them. Finally, the very fact that computers present a highly visible target in both a physical and a political sense can be of benefit to those seeking ways to protect privacy.

Closely related to security is the question of carelessness. Invasions of privacy may occur as readily by default as by design: examples include sensitive files left lying around for strangers to see; researchers who talk too freely about the individuals whom they have interviewed; census enumerators who gossip about the data they collected from a house down the street. Training and monitoring of databank personnel are means of minimizing security "leaks" through carelessness.

5. Data Dissemination

The criteria governing the persons or institutions to whom data may be disseminated, the terms and conditions under which it is disseminated or exchanged, and distribution practices vary among different databanks. A few databanks, Statistics Canada is an example, are forbidden by law to distribute or publish any information about identifiable individuals. In the private sector (and in the public as well, in the instance of one provincial motor

vehicle licence bureau), some databank operators, presumably on the grounds of a supposed proprietary right, consider themselves justified in making the contents of their files available to third parties. Such operators regard this as a matter entirely for themselves to determine. As a consequence, individuals who may divulge information about themselves in order to achieve a particular benefit or to fulfil a requirement (for a licence or a lease) may then discover – or worse, not discover – that this information has been used by third parties in a wholly different context. Thus a name and address given for one purpose may find itself passed along on a mailing list to be used to solicit business. A medical record – if it is exotic enough – may find its way into the medical lecture room. Government agencies bear a particular responsibility to be careful about their dissemination practices since they frequently collect information under statutory authority. In general, governments are by far the largest collectors of data, all amassed in the name of "the public interest". In the public interest, also, governments have a particular responsibility to ensure the confidentiality of such information.

Most databank operators collect their information from the individual concerned, who either provides the information himself or authorizes its collection. In these cases, until this information is passed on to a third party, particularly another databank operator, the individual can be said to know the purposes for which the information about himself was collected and the uses to which it is put. However, once the information passes to a third party – even with the individual's awareness or authority, but certainly without it – he loses this knowledge, along with a sense that he has been in control of the information about himself.

The entire question of personal-data dissemination would appear to be one which requires careful attention and calls for some guidelines, such as those in the Manitoba Personal Investigations Act.

6. The Question of Access

On the question of whether individuals should have access to their own files, a gamut of attitudes is discernible. According to the Task Force survey, most databank operators agree that individuals should have the right to know both of the existence of a file on them and the contents of the file, despite the fact that this "right" has so far not been extensively honoured. It is only recently, for example, that credit bureaux have made it a general practice to

permit individuals to see their files although this is now compulsory in Quebec, Saskatchewan and Manitoba.

Attitudes begin to differ on the question whether the individual should have a right to put on the file any rebuttal he may have about facts contained in the file (a right also recognized in the above-mentioned provinces), and whether he should have a right to insist on corrections, clarifications, deletions, or additions.

Attitudes differ also on the question whether the data subject should be informed each time information on the file is passed to a third party and who the third party is, and ultimately, whether he should have the right to consent to the onward distribution. Finally, opinions differ on whether the individual should have the right to know the sources of the information about him.

The Task Force recognized that the conditions of access can cause difficulties. The cost of exercising the right may be set at a prohibitive level, and it is of little use for an individual to be shown a printout of his file in which all the information is encoded into alpha-numeric symbols. In addition, demands for access can become excessive. Proposals have been advanced that would require the operators of databanks to dispatch regular file printouts to all subjects. It is quite possible, however, that few individuals would want to verify their own files.

The important and controversial issues raised by the question of access should be fully explored and resolved with a view to ensuring that a right of access by an individual to his file is recognized in principle and realized in practice to a degree sufficient to protect his privacy and related interests. Different types of files will require different solutions.

7. The Politics of Privacy

Throughout this Report, an attempt has been made to suggest that certain interests, claims and values, such as confidentiality, are directly related to privacy, while others such as accuracy, which although emotionally and practically related, are conceptually distinct from privacy as such.

Beyond using the word "privacy" to refer to the entire range of these specific concerns, regardless of whether they are directly related to the concept of privacy or not, some participants in the computers-and-privacy debate make very liberal use of the word to denote a much broader and more fundamental type of concern. Here privacy is used essentially as a synonym for a cluster of social

grievances and frustrated political expectations in a society that is complex, institutionalized, and impersonal.

A clue to the nature of these concerns is provided in the statement of Professors Weisstub and Gotlieb, in their Study for the Task Force, that "privacy is power." This is of course a play on the observation that "information is power." In the post-industrial society, emergent or already emerged, information holds a central place. It can be a key to decision-making: those who have it make decisions, those who lack it may be inhibited in the making of decisions and may also be prevented from participating in the making of decisions about them by others. Privacy thus becomes a surrogate name for generalized concerns, often inarticulate and ill-expressed, that vary from worry about the amount of personal information being collected to a fear that the possession of this quantity of information will greatly extend the powers of manipulation and enforced conformity exercised by those who control the information.

An analogy can be drawn from the contemporary debate over environmental pollution. The scale of protest may there indicate a concern not just with the state of the physical environment but also with the state of a social and political environment which emphasizes profit to the detriment of pleasure.

Analogies can be invidious, particularly one drawn from so emotive a subject as environmental pollution. Nevertheless the parallel may be useful to the extent that it reveals that the debate over privacy in part may be miscast. Individuals may be concerned no so much that their privacy will be invaded in the classic sense as that it, and their individual freedom and autonomy, are in danger of being eroded by the existence of massive and highly efficient information systems.

Computers have attracted so much attention that it is worth recalling that the explosion in information-gathering long preceded their invention and application. Governments initiated the first universal data-gathering exercises to collect taxes and suppress rebellion and, much later, to administer welfare and income redistribution programs. The private sector, once it recognized the commercial value of accurate and readily available information, provided the second principal source of demand. More recently, social scientists, in company with market researchers, have precipitated a third wave of data collection and analysis.

All this ravelling up of information has produced an industry that has now reached staggering proportions. At the same time a second, and to a degree opposed, trend is making itself felt. As

Weisstub and Gotlieb comment, "The expectations of modern man for increased knowledge have reached unmanageable proportions." Individuals, in short, have enormously raised their expectations about what it means to be an individual. This development has taken place at a time when institutions, as a consequence of programs designed to benefit individuals, have acquired enormous amounts of information about individuals (and about things), which can then be used to serve the interests of these institutions.

This Report is not the place to attempt an analysis of organizational behaviour, nor to question whether institutions, however benevolent their origin, may tend after a passage of time to manufacture new needs in order to justify their existence and expansion. The simple observation that such suspicions are being voiced more frequently, and certainly more loudly, is unarguable. In such an equation the role of information is critical. Information systems appear to enhance the efficiency and therefore the power of the institutions that operate them. Those who question the authority of those institutions, or at least the ways in which that authority is exercised, may attack their behaviour on the grounds that it invades privacy, when in fact the real target is institutional power and its linkage to the possession of information.

Less critical, but also revealing of the nature of the debate, is the role of computers. The fact that the issue is so often raised under the banner of "computers and privacy" rather than of privacy alone is instructive. Computers are most efficient when dealing with information that can be quantified and systematized; information that is intuitive, ambiguous, emotional is much more difficult to computerize. As a consequence computers may reinforce the importance in the decision-making process of the technocrat over the humanist, the objective over the subjective. As one illustration of their potential political effects, A. Downs[1] notes that as a result of the growing use of computers:

> "The government bureaucracy as a whole gains at the expense of the general electorate... well-organized and sophisticated groups gain power at the expense of the less well organized... technically-educated officials gain power at the expense of old-style political advisers."

Non-organized, non-technocratic individuals – which is another way of saying most people – could be disfranchised by the rise of this type of decision-making.

All this adds up to a presentiment of a technocratic nightmare, which is not only over-simplified, but speculative. What computers may do and what they actually do are quite different. With few

exceptions, perhaps as in multi-national corporations, computerized information systems and particularly the much heralded Management Information Systems (MIS) have made little difference to organizational behaviour. Generally, MIS systems, as the Computer/Communications Task Force found, have fallen far short of expectations. As important, computers can, if the political will exists, make the same information available to everyone.

This description of privacy has cast it in the role of a synonym, or symbol, for a cluster of societal concerns, all related to the possession of information or to the denial of it. Those concerns in turn seem to be rooted in premonitions of impotence in the face of all-knowing institutions, of manipulation, of being reduced to a cipher, of being pressured to conform.

One of the commonest proposals advanced by those concerned with the political aspects of the privacy debates is that individuals should have not only a right of access to information stored about them; but, as a means to secure a better balance of power in society, should also have a right to information about the institutions that confront them. Some militants would go even farther, and have argued that their goals would be best achieved if all privacy were abolished, that of institutions as well as that of individuals, so that information and hence political power would be evenly spread. As Claude Fabien noted in his Study for the Task Force:

> "L'objectif du contrôle des agents agresseurs de la vie privée, c'est ultimement d'atténuer ces frustrations, de diminuer les tensions qui en résultent entre l'Etat et le citoyen, entre l'organisation économique et le consommateur, entre l'employeur et l'employé. L'objectif, c'est en réalité la paix sociale."*

8. Freedom of Information

The preceding section has raised the question of access by the individual to information in the hands of institutions as a means of securing a better social balance between individuals and institutions. Not surprisingly, the public increasingly demands information from government and business to ensure their accountability to the people and to increase the latter's participation in the regulation of public affairs.

*Editor's translation: "The ultimate goal in controlling those factors which work against individual privacy is to decrease these frustations, to reduce tensions between state and citizen, business and consumer, employer and employee. In essence, the goal is social peace."

But while the individual, as a member of the public, seeks "freedom of information" or the "right to know", in his personal life he claims a right to privacy. Some accommodation between these two interests, therefore, must be made. If the privacy of the individual is to be protected, there will be occasions when information cannot be divulged. In other situations, personal information about an individual may be of such vital concern to society that the individual's privacy must be sacrificed.

It is not always true that one or other of these twin rights must prevail in any given circumstance. Various situations may permit more subtle differentiation giving each of these rights some recognition. For example, governments and business organizations may, in the interests of social planning or efficiency or other social needs, be justified in obtaining information on a wide variety of matters even though the individual may consider it sensitive or closely related to his economic interests. It by no means follows, however, that government and business are justified in making this information available to the public in the name of some abstract notion of "freedom of information." Again, a member of the public may have a legitimate interest in gaining access to a document or government file containing information of personal interest to him, but this interest may have to be balanced against that of others where the document or file also contains personal information about them or sets forth their personal opinions.

From these examples it is obvious that the inevitable tensions between "freedom of information" and the "right to privacy" cannot be resolved in terms of abstract formulae. Rather the task demands a sensitive balancing in the context of particular situations. It may well be possible to devise guidelines to assist in the resolution of such issues, but this was beyond the purview of the Task Force. The task of sorting out when and under what conditions one or other right should prevail will be assisted by the elaboration of a general policy on "freedom of information".

9. Summary

Political issues lie beyond the competence of the Task Force, although an appreciation of the underlying unease about pervasive, efficient information systems (quite apart from whether their operations involve actual invasions of personal privacy) helps to explain the persistence of public interest in the issue of informational privacy.

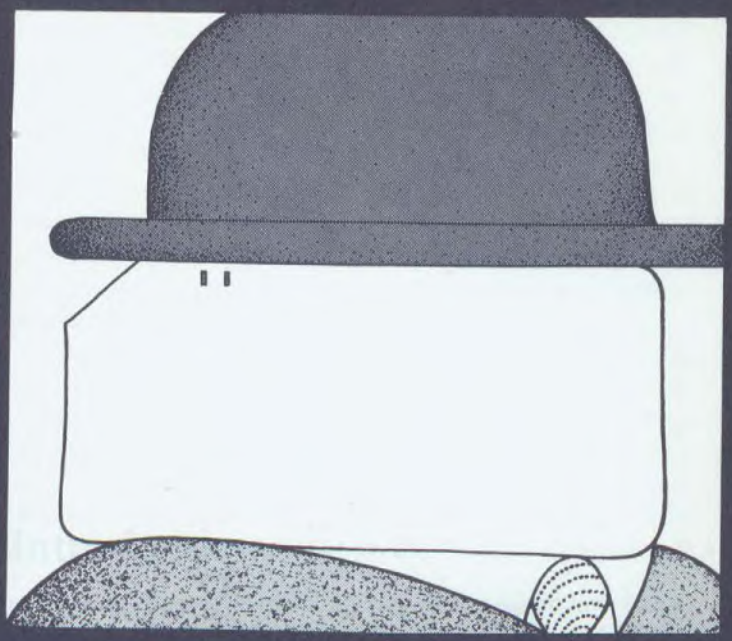
The more immediate focus of the Task Force is that of the

specific concerns to which information systems give rise. Accuracy, relevance, control over distribution, security standards, the provision of opportunities for access, and guidelines for collection procedures, appear to the Task Force to be matters that require some form of regulation in respect of databanks that contain sensitive information about identifiable individuals.

The Task Force believes that particular note should be taken of the finding, derived from the replies to the privacy questionnaire, of the general readiness on the part of operators of databanks to accept some reasonable safeguards for privacy. This finding may indicate a concern about possible threats to privacy, shared by databank operators who, as individuals, are the subjects of someone else's databank. It may equally indicate a pragmatic willingness to accept minimal standards as a price for defusing public debate. In either event, an unexpected responsiveness appears to exist.

[1] Downs, A., "The Political Payoffs in Urban Information Systems", in Westin (ed.), *Information Technology in a Democracy*, Harvard: 1971, pp. 311-21.

Section V



Privacy and the Law

Chapter 11
The Law Relating to Privacy of Information

1. Introduction

In examining the treatment of privacy in Canadian law, one is struck by how rarely claims to privacy have been advanced before the courts. This may come as a surprise to those who place emphasis on legal solutions in the computers-and-privacy debate. All the more so because it is in marked contrast with the state of the law in the United States, a country with which we share a wide range of values.

In the United States, which has a common law system similar to that in nine of the ten Canadian provinces (the exception being Quebec where the Civil Code governs), the courts have developed a considerable body of law relating to privacy during the eighty-odd years since the famous article by Warren and Brandeis on the right of privacy appeared in the Harvard Law Review of 1890.[1] This situation should not, however, be cause for too much surprise. As Roscoe Pound has noted of such social interests as privacy, "the law does not create these, it only recognizes them."[2] Before the law

will respond to a social claim, there must be some social recognition of its validity.

As we have seen, claims to privacy have become insistent only in recent years, largely as a by-product of our urban, and more particularly of our post-industrial society. In a predominantly rural society, a significant part of one's life was lived alone with one's family and neighbours, free from the close scrutiny of outsiders. What were considered invasions of privacy amounted largely to intrusions on the enjoyment of one's property, home life and reputation. In this context the law responded, largely through the laws of trespass, nuisance and defamation, to protect the setting in which home and social life took place.

The issues of privacy of direct relevance to the Task Force, however, are related to the anxieties about personal information that may be cast without a person's knowledge into the flow of commerce or the government apparatus – quite possibly to be used against his interests.

The fact that the United States became highly urbanized and industrialized long before Canada may explain in part that country's lead in developing privacy as a legal concept. Yet, this cannot fully account for the matter. For our common law is largely based on that of Great Britain, which has long been a highly urbanized country. Consequently other reasons to explain why development of the law relating to privacy in Canada may have lagged behind that of the United States must be canvassed. It may simply be owing to the somewhat different social situations in the two countries; for the general *mores* of a people have an important role to play in the development of the law. Not the least of these differences is the attitude towards law and the courts as an instrument for resolving disputes on social issues. In the United States there is greater reliance than in Canada on the judicial process for the settlement of such disputes, coupled with marked judicial innovation, which is partly the cause and partly the result of this reliance on the courts. This legal development has been fortified by the pervasive influence of the United States Constitution, which incorporates many of the fundamental values of that country, including a number of rights relating to privacy. Canadian constitutional instruments, by contrast, are almost exclusively confined to delimiting areas of government power.

As outlined in Chapter 1, privacy may be regarded as a constellation of three realms or zones in which an individual may, as a function of his personality, claim to be let alone to do as he sees fit. These relate to territorially definable zones in which an

individual may seek to be physically removed from and undisturbed by others, the zone occupied by his body which the law has surrounded with an aura of inviolability, and the intellectual zone where he may seek to prevent information about himself from passing into the knowledge of others, particularly by such illicit means as eavesdropping. All three of these claims, of course, are subject to counterclaims.

The Task Force was particularly concerned with the third sense of privacy – in the context of the gathering, storing and dissemination of information about a person.

Two stages in the information process identified earlier in the Report correspond roughly to what the computer jargon refers to as "input" and "output". The first is the data-gathering phase, a stage at which privacy is brought into play as facts about an individual are taken from his private zone and passed on to another. It involves questions of how and what types of data are gathered. The second and more important stage in terms of the Task Force's concerns is that of data dissemination, when personal data may be passed on to others deliberately or inadvertently as a consequence of inadequate security.

Both the common law and the Civil Code systems respond to new social claims in terms of their respective underlying principles: the common law by adapting existing remedies to new situations and occasionally by evolving new ones; the Civil Code system by applying principles (such as those relating to delicts, i.e., wrongful acts) to new fact situations. Each system in its own way attempts to adapt and to stretch the existing law to respond to new social claims as times and values evolve and change.

Canadian law does not recognize a general right of privacy although, as will be seen, there are interesting developments particularly in British Columbia, Manitoba, Saskatchewan and Quebec. Further, there are areas of the law that indirectly protect privacy. To say, therefore, that privacy is not at present a generally recognized right under Canadian law, is by no means to imply that no legal protection exists.

In the widest sense, it can be argued that many civil rights, whether real or personal, imply a recognition of privacy because they affirm an individual's capacity to exercise personal choices, such as keeping others off his property, engaging in contractual arrangements with others, and so on. In a narrower sense, there are specific rights and remedies that relate to spheres of interest involving privacy. These interests are protected by civil actions for acts such as defamation and breach of confidence, by criminal laws that

prohibit certain violations of an individual's dignity and reputation, by the laws of evidence which protect the confidentiality of personal information arising out of certain relationships, as well as by various statutes that create penalties for divulging information except as legally authorized.

2. The Data Gathering Phase

In confronting a data collector seeking information about him, a person can, of course, refuse to divulge it. In some instances, such as applying for a passport, or for insurance or for credit, an individual is under no legal obligation to provide the information required, but the consequence of his refusal would usually be to forego the benefit being sought. In other cases the law may actually require divulgence of the information. Examples are search warrants, federal and provincial Income Tax Acts and the Statistics Act.

Other statutes protect the individual against certain unlawful extractions of information. Important general statutes exist in Manitoba and Saskatchewan but these will be more fully discussed in relation to data dissemination, which falls more squarely within the concerns of the Task Force. In Ontario, legislation imposing strict licensing requirements on private investigators was enacted in 1965.[3] However, this statute does not apply to:

> "persons who search for and furnish information (i) as to the financial credit rating of persons, (ii) to employers as to the qualifications and suitability of their employees or prospective employees, or (iii) as to the qualifications and suitability of applicants for insurance and indemnity bonds, and who do not otherwise act as private investigators."

Specific legislation prohibits unlawful interference with communications and surveillance of individuals. Thus section 9(2) of the federal Radio Act[4] prohibits the unauthorized interception of radiocommunications (although the offence is actually committed by using or divulging the unauthorized message). This section, among its other functions, implements for Canada an undertaking under the International Telecommunication Convention respecting the secrecy of telecommunications. Again, the Bell Canada Act[5] prohibits the interception of telephonic communications. Similar provisions exist in Alberta, Manitoba, Ontario, Quebec and Nova Scotia. And, subject to certain exceptions under the Penitentiary

Act, present Canadian law appears to place a categorical prohibition on the deliberate interception or opening of letters, including by police or government agencies.

The recently introduced federal Protection of Privacy Bill[6] would prohibit the unauthorized interception of a "private communication" by electro-magnetic means, including bugging and wiretapping, as well as by acoustic, mechanical or other devices. A private communication is defined as an oral communication, or any telecommunication made under circumstances where it is reasonable for its originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it.

Related to the question of wiretapping is that of eavesdropping and peeping-Tommery. The Criminal Code[7] prohibits prowling or trespassing at night and "watching and besetting" but these would not, for example, cover the cases of spying on a neighbour from one's own property by means of a long-range telescope, or of a landlord spying on his tenants. These intrusions on privacy are not expressly prohibited except possibly in British Columbia and Manitoba, where the invasion of privacy has been made actionable *per se*.[8] However, protection may at times be afforded under the general law, where, for example, such an act amounts to trespass, nuisance or negligence.

3. The Data Dissemination Phase

The Task Force was primarily concerned with the dissemination of information to third parties. While there are some statutory provisions affecting the matter, notably in British Columbia, Manitoba and Saskatchewan, the general remedies in the Civil Code and the common law afford the principal protection to privacy in this context. In the following discussion an attempt is made to highlight the civil and common law remedies related to privacy which at present afford it protection.

a. The Civil Law of Quebec

Under Quebec law, it is not necessary to think in terms of a list of particular wrongs into which factual situations must fit if there is to be a legal remedy. Rather, it is necessary to determine whether general principles of delict, based on the notion of fault, apply to the particular situation.

A remedy will lie against an individual if his conduct has been

such as to constitute a wrong within the terms of the Civil Code of Quebec, particularly Article 1053, which reads as follows:

> "Every person capable of discerning right from wrong is responsible for the damage caused by his fault to another, whether by positive act, imprudence, neglect or want of skill."

This Article has permitted a good deal of flexibility in ascertaining whether new activities (such as those produced by new technological developments) are wrongful or not and in creating rights and obligations related to them. In respect of privacy, Quebec law produced a significant legal decision as early as 1957. In *Robbins v. Canadian Broadcasting Corporation,*[9] an announcer read on the air a letter from a Dr. Robbins complaining about the station's programming and concluded by suggesting that viewers "cheer up" the writer, whose name and address were flashed on the screen. In consequence, Robbins received unwanted grocery deliveries and was harassed in various ways. The C.B.C. was held liable because the court found its conduct to be wrongful. The act of broadcasting the letter sent by Robbins invaded his privacy by identifying him and publicizing his personal views. A number of writers have argued that this case established a general right of privacy in Quebec.

More traditional applications of Article 1053 may also serve to protect privacy. Thus there are remedies for defamation and for breach of confidence similar to those discussed in the context of the common law.

b. The Common Law

The common law may, in time, give birth to a new general tort of privacy. At this point, however, the major areas of the common law most directly concerned with the protection of privacy of information are defamation and breach of confidence. Both relate directly to situations where information about an individual is communicated and he objects to this communication.

Defamation is a tort (or civil wrong) that protects a person against communications that tend to detract from his good reputation. It is relevant to privacy because it is concerned with the dissemination of information about an individual. Moreover, it is a tort that can frequently be relied on in this type of privacy case. However, because it relates to *false* information, it does not strike at the heart of the privacy concept because it does not protect an individual against the dissemination of truthful facts about him

(irrespective of the harm which may accrue as a result). Publication of truthful facts – though not deemed by law to be defamatory – may still invade privacy.

This tort presumes that a man's reputation affects his relations with others and seeks to compensate him to the extent that these relations are harmed by damage to his reputation. It protects a person's pride and self-respect insofar as they derive from others' conceptions about him. It is not the indignity or the outrage of a lie (a slander when spoken and a libel when written) but the damage that it causes to reputation that is essential to the tort. On the other hand, there have been many awards of exemplary damages to compensate for just this outrage and indignity once defamation has been found.

Credit reporting illustrates some of the limitations of defamation as a remedy against the invasion of privacy in the information context. Credit reporting agencies market information about people which is used as the basis for decisions on whether or not they are worthy of credit. They deal in purported facts, some directly tied to a person's financial affairs, such as his income and debts, others related to personal characteristics that may have something to do with financial responsibility and reliability.

What makes credit reporting objectionable at times, and raises questions of possible invasions of privacy, is the fact that the information may be incomplete, irrelevant, inaccurate and possibly damaging, and that the individual may be totally unaware of when, how and by whom the reports are being made. Of all these sources of concern, defamation can at best deal only with the question of the accuracy of the information, where inaccuracy amounts to untruth and where one is certain that the information was in fact transferred, both of which are far from easy matters to determine. If nothing false is included in the report on an individual, the tort of defamation provides no remedy however much he is in fact aggrieved or even harmed. It provides virtually no obstacle to a credit reporting agency disseminating truthful information whenever and to whomever the agency pleases and regardless of whether or not the subject of the information knows of the dissemination. (Another remedy that might possibly be available in these circumstances is the embryonic tort of negligent misstatement referred to later.)

Still the mere existence of the tort of defamation may inhibit the spread of damaging information (and so protect privacy) because of the danger that an action might be brought if information thought to be true turns out to be false. This is accentuated by

the fact that some cases have tended to widen the protection afforded by the tort by requiring that statements that discredit people be not only substantially, but exactly true. This has a tendency to discourage derogatory statements. In the case of *Green v. Minnes,*[10] for example, a debt collector posted a conspicuous yellow poster in various parts of the city advertising that the plaintiffs owed a certain amount of money. This was substantially true (as a lower court had held). However, the appeal court unanimously held that because the amount claimed to be owing on the poster was not strictly correct, the tort of defamation had been committed. It appears clear from the judgment that what activated the court was its disapproval of the method of collection employed, namely the publication of harmful information.

Moreover, the courts have held that if information is untrue, a private credit agency cannot rely on the defence (known as qualified privilege) that it has a duty to disclose the information to its clients. (This is one area where Canadian law may be more protective of the individual than that of the United States, where qualified privilege is often a defence). But if a private credit agency cannot rely on this defence, the credit departments of two companies in the same line of business may be able to do so. Often one company tells another about its dealings with a particular customer and these communications may come within the defence of qualified privilege unless the statement is malicious.

In summary, the tort of defamation may continue to provide one approach to the protection of privacy. However, the conceptual difference between reputation and personal integrity is likely to limit the usefulness of defamation in protecting the privacy of information about a person. A man's reputation is essentially based on the assessment and esteem of others. His personal integrity is fundamentally a matter internal to himself and relates to his self-esteem. Reputation is legally recognized to be injured by falsehood or malice. Personal integrity may be injured merely by facts about an individual passing out of his control. The invasion of privacy may thus not be defamatory; defamation, although it may cause an individual anguish, need not invade his privacy.

It is worth noting that defamation is also a crime in Canada. It differs from the tort in that truth is not necessarily a defence. Thus, for example, if a credit reporting agency issued a damaging report about a person seeking credit, this person could, theoretically, prosecute the agency because of the damage he suffered and a guilty party could be imprisoned for up to two years. On the other hand – and even if the report is false – case law has determined

that the employee of the agency will not be criminally liable for this defamatory act if he was not motivated by "ill-will", if his conduct was reasonable in the circumstances, and if the recipient of the report had a legitimate interest in receiving it.

Individuals, in the course of their lives, enter into a variety of relationships with others in which information is imparted or exchanged. In certain cases this information is acknowledged by society and by law to be confidential. Accordingly, the law places a kind of protective wall around the information, restricting it to the parties concerned.

The question of the divulgence of confidential information frequently arises in relation to the evidence that may be advanced in court. Under both federal and provincial laws of evidence, discussions between husband and wife and between solicitor and client are privileged and need not be divulged in testimony. Similar protection is afforded to other relationships under various provincial statutes. Further, information acquired by the Crown may be kept private if the trial judge considers that it is in the public interest to do so.

A second way the law protects confidentiality is through freedom of contract. Thus, an individual can assure privacy by making confidentiality a condition of contract. For example, if a man who is in debt is forced to sell his house, he might be able to stipulate that this fact be held confidential under penalty of breach of contract. The contractual area of confidence can be as wide as the parties agree.

Beyond express contractual relationship, the courts have shown a willingness to find an implied contract or obligation of confidence in certain situations. Thus, as early as the 1888 case of *Pollard v. Photographic Co.*,[11] a photographer was restrained from selling or exhibiting photographs of a lady who had paid him to photograph her partly on the grounds that there existed an implied contract not to use the negatives for such purposes and partly because he had abused "the power confidentially placed in his hands merely for the purpose of supplying [a] customer." This reasoning might equally be applied to situations where a person confides information to another for one purpose and it is disseminated to third parties for other purposes.

But a broader protection of confidentiality exists in the equitable jurisdiction of the courts. Whenever a confidential relationship occurs, the courts will intervene to prevent abuse of the confidence by one of the parties. The confidentiality of the relationship may arise from numerous sources: status (as between husband and

wife), contract (as between doctor and patient), or under statute (as in the federal and provincial Income Tax Acts). Indeed, the courts have been willing to protect confidential relationships even in the absence of one of these three sources of confidentiality. For example, in the 1948 English case of *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.*,[12] the defendant company made certain tools for its own use from drawings furnished to it by the plaintiff company on a confidential basis. Even though no contract existed between the two companies, the court held the defendant liable for breach of confidence. One of the judges, Lord Greene, formulated this principle:

> "The obligation to respect confidence is not limited to cases where the parties are in contractual relationship .... If a defendant is proved to have used confidential information, directly or indirectly obtained from a plaintiff, without the consent, express or implied, of the plaintiff, he will be guilty of an infringement of the plaintiff's rights."[13]

The law's capacity for growth in this area can also be seen in the 1965 English case of *Argyll v. Argyll*,[14] where the court went beyond the protection previously accorded to communications between husband and wife. There the wife obtained an injunction to restrain her former husband from publishing confidential matters about their married life. The court made it clear that it was not relying wholly on existing precedents but was basing its decision on the general "policy of the law":

> "If this were a well-developed jurisdiction, doubtless there would be guides and tests to aid the court in exercising it. If, however, there are communications which should be protected and which the policy of the law recognizes should be protected, even to the extent of being a foundation of the old rule making husband and wife incompetent as witnesses against each other, then the court is not to be deterred merely because it is not already provided with fully developed principles, guides, tests, definitions and the full armament for judicial decision. It is sufficient that the court recognizes that the communications are confidential, and their publication within the mischief which the law as its policy seeks to avoid, without further defining the scope and limits of jurisdiction: and I have no hesitation in this case in concluding that publication of the passage complained of would be in breach of marital confidence."[15]

Although the two cases just cited are English, similar principles apply in the common law jurisdictions in Canada. Equitable relief generally takes the form of an injunction, in this case preventing a person from wrongfully using or disclosing information obtained in confidence. However, damages may be awarded in addition to or in place of an injunction. Such equitable damages are rare, but may be useful to compensate for an invasion of privacy. This step could be taken where information has been used for purposes other than those for which it was originally collected. Indeed, equity may be particularly useful in protecting privacy because "the court in the exercise of its equitable jurisdiction will restrain a breach of confidence independently of any right at law."[16]

Statutes requiring the divulgence of information often recognize its confidentiality. Perhaps the most stringent protection of this kind is contained in the federal Statistics Act,[17] which strictly prohibits the disclosure of any information obtained under the statute, or the use of information to identify particular individuals. The federal Income Tax Act[18] also prohibits the dissemination of information to any person not legally entitled to it. However, such prohibitions usually appear only in laws requiring specific facts to be reported.

On the other hand, no general guidelines regulate what information may, under law, be collected by governments. The invasion of privacy occasioned by the collection of data may be compounded where the facts collected are irrelevant to the stated objectives of the law, all the more so if they are later used for other purposes. Often, statutes authorize schemes (for example, welfare plans) whose administration requires the collection of information about individuals. Although the oath of office taken by all public servants and the general law governing breach of confidence may prevent dissemination of such information, there may be no legal avenue to prevent its accumulation. Moreover, except as regards sensitive information, the rules governing the occasions when and the conditions under which personal information may be disseminated within the public service do not appear to be fully adequate. The foregoing considerations apply with greater force to private organizations such as credit bureaux, for they are not subject to many of the rules existing in government.

Apart from defamation and breach of confidence, negligence and the principle enunciated in the case of *Wilkinson v. Downton*[19] may, on occasion, provide some protection for privacy of information.

The relevance of an action for negligence to information systems and privacy lies in the fact that it is the most general remedy in the law of torts today. It is available whenever a court finds that the defendant has a duty of care in the circumstances and that his negligent conduct has caused the plaintiff damage. It might cover the case where a databank operator possessing damaging information about a person negligently allows its dissemination.

Again the related tort of negligent misstatement might be expanded. This tort will cover the situation, for example, where a bank gives a wrong credit reference about a customer who later goes bankrupt. The person who gave credit to the customer will have a remedy. Thus far, however, the tort has only given a remedy to a plaintiff who acted upon the information to his detriment.[20] It has not yet been extended to the opposite situation, where the customer has suffered the loss, but this may, in time, occur.

A more remote possibility is the principle in *Wilkinson v. Downton,* where the court held that liability in tort may be imposed for any intentional act that results in harm. Though little used, the principle might have some applicability in relation to certain activities related to information collection and dissemination. It was applied in *Janvier v. Sweeney*[21] where the defendants, private detectives, had sought to obtain information about the plaintiff's employer by threatening that they would reveal damaging information about the plaintiff's fiancée. As a result of the threat the plaintiff suffered nervous shock and recovered damages from the defendants.

4. The Relevance of the Law of Property

It was noted earlier that the law may be interpreted as recognizing certain zones of privacy in relation to a person's property and to his physical person. Certain protections of privacy in relation to property are also important in relation to the gathering, handling and transfer of information about him. Moreover, the protection afforded privacy in relation to one's property suggests the notion of a core of privacy.

The physical or territorial zone of privacy has historically been defined in terms of the law of real property. In great measure, legal protection of the individual's enjoyment of property is to be

found in the torts of trespass and nuisance in common law jurisdictions, in the law of delicts in Quebec, as well as in certain provisions of the criminal law.

An action for trespass may be brought for the unlawful presence of a person on another's land. Technically it does not require an individual to prove that damage has resulted from the trespass. Courts, it is true, will only award nominal damages for trivial disturbances, but a significant invasion of privacy will not be regarded as trivial. Privacy is further protected by the Criminal Code which makes various physical penetrations of a house or land, such as housebreaking and trespassing at night, punishable offences. A physical zone of privacy in which an individual may be protected is thus delineated.

The tort of trespass tends to protect privacy of information by keeping people physically away from sources of information. But it does not extend to all invasions of informational privacy. For example, if an intruder in a person's house discovers certain facts which the owner considers private, such as his membership in a political party which the intruder learns by finding his membership card, a loss of privacy will be an effect of that trespass, but will not be covered by the tort. This, of course, does not rule out other remedies (such as, for example, an action for conversion or prosecution for theft, if the intruder wrongfully appropriates the card). Moreover, equitable principles, increased damages and criminal proceedings might be appropriate responses to such invasion of intellectual privacy.

There are, as well, instances outside the field of property where the provision of physical privacy is intended to protect the privacy of information. Well known examples are federal and provincial statutes guaranteeing the secrecy of ballots in elections by establishing total privacy in the polling booth.

With respect to the laws governing the search of premises, the recent New Brunswick case of *Re K.C. Irving Ltd. v. The Queen*[22] highlighted the relevance of considerations of privacy that reach beyond the property context to the informational. In that case, combines investigation officers had, under warrants duly issued, searched the homes of three individuals in order to obtain certain information relevant to a charge of violating the Combines Investigation Act which they suspected might be hidden there. The court held that the issuing and execution of these particular search warrants constituted an invasion of privacy, since the warrants had been issued without reasonable grounds for believing that the individuals were concealing or were likely to conceal evidence.

Similarly, the laws dealing with searches of the person also protect privacy. Under the Criminal Code, a personal search of an individual can be made by a policeman only under certain circumstances – where he has valid reason to believe that the individual has, or is about to commit a crime. Otherwise, a search of a person even by a policeman is an assault punishable as if committed by anyone else. To the extent that the crime of assault involves indignity as well as physical harm, it protects privacy in the intellectual sense as well as the physical.

The responsiveness of courts to claims to personal privacy is evident in various parts of the law. For many years, the common law has recognized that an individual has a legal interest in such personal matters as his name, likeness and the contents of personal letters.

The spirit of the law is well exemplified in the case of *Williams v. Settle*.[23] There the defendant, a commercial photographer, was engaged to take photographs at the plaintiff's wedding. Some time later the plaintiff's father-in-law was murdered and two newspapers persuaded the photographer to sell them a picture of the wedding group, which was then published. The plaintiff's suit succeeded on the ground that the plaintiff owned the copyright in the picture. It is true that the plaintiff could not have succeeded if the copyright had belonged to the photographer (and not the plaintiff), but as the Pollard case discussed earlier demonstrates, the courts can be astute in finding a remedy. The court in *Williams v. Settle* went on to award exemplary damages because of the personal values infringed. Sellers J. stated:

> "it is sufficient to say that it was a flagrant infringement of the right of the plaintiff and it was scandalous conduct and in total disregard not only of the plaintiff's legal rights of copyright but of his feelings and of his sense of family dignity and pride. It was an intrusion into a man's privacy, his life, deeper and graver than an intrusion into a man's property."[24]

From cases such as these, scattered in various areas of the law, it is possible that the courts may find it necessary to develop a comprehensive remedy for the protection of privacy, though this, of course, is by no means certain.

5. Specific Statutory Remedies for Invasion of Privacy

Two provinces have decided not to wait for the gradual evolution of doctrines for the protection of privacy by the courts, and have enacted statutes declaring a general right of privacy.

British Columbia was the first province to enact a Privacy Act, in 1968.[25] The Act makes it a tort, actionable without proof of damage, "wilfully and without claim of right, to violate the privacy of another" (s.2) or to make use of a person's name or portrait (including impersonation or caricature) without consent for the purposes of trade or commerce. According to s. 2(2):

> "The nature and degree of privacy to which a person is entitled in any situation or in relation to any matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of another, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties."

So far only one action has been brought under section 2.[26] There the plaintiff became ill as a result of knowing that he was being watched and followed. It was held in the first instance that this surveillance was an actionable tort under the Act. However, on appeal it was decided that the defendant was not in breach of the Act because the surveillance was "reasonable" and because the worry, apprehension and emotional upset of the plaintiff were not relevant to the question of whether his privacy had been violated.

Manitoba also has a Privacy Act, which came into force in 1970.[27] Like the British Columbia legislation (although the difference in phraseology is worth noting) the Act makes it a tort, actionable without proof of damage, "substantially, unreasonably, and without claim of right" to violate the privacy of another (s. 2). Section 3 provides non-exclusive examples including surveillance of any kind, intercepting telephone conversations, unauthorized use of name, likeness of voice for purposes of gain, unauthorized use of personal documents. These examples suggest that the Act may go further than the British Columbia Act towards protecting the individual. Neither Act defines privacy, however, except in a negative sense.

Both of these Acts appear to be aimed mainly at discouraging

unsavoury methods of collecting information and its unauthorized use by the media. Other provincial legislation, in Manitoba, Quebec and Saskatchewan may be more relevant to the problems considered by the Task Force.

Probably the most sweeping legislation affecting private information systems is the Manitoba Personal Investigations Act of 1971.[28] With certain important exceptions, including provincial and municipal governments and their agencies, the Act requires that: the person being investigated either consent to such investigation or be notified of it in writing; certain kinds of information (e.g., as to race, ancient legal history, uncorroborated investigative information) shall not be included; information contained in a personal report shall not be divulged except in specific circumstances; the subject of a report shall be entitled to see it and to be informed of the source of the information in it; the subject may protest any inaccuracies disclosed. The statute is penal in nature and no civil liability is imposed except in cases of malice or negligence.

In Quebec, sections 43 to 46 of the Consumer Protection Act (1972)[29] provide some relief for the subjects of credit reports by enabling them to examine and obtain copies of reports concerning them and to register their comments on the report. There is, however, no restriction on the type of information that may be collected or the use to which it may be put. And there is no means of ensuring that corrections reach those persons who may have received an erroneous report.

The Quebec Public Protector Act (1968)[30] may provide relief where damage to individual privacy has been caused by a public servant. Section 13 simply states that:

> "The Public Protector shall make an investigation upon the application of any person whenever he has reason to believe that in the exercise of an administrative function the holder of any position ... under the government ... has wronged such person."

Other provisions also protect the confidentiality of information required by the Public Protector in the course of his duties; in particular, he cannot be compelled to reveal such information by the courts.

Finally, the Saskatchewan legislature passed an Act in 1972 (to become effective in 1973) to regulate credit reporting agencies. The Credit Reporting Agencies Act[31] prohibits the operation of such agencies without a license and attaches conditions to the obtaining and renewal of licences. In particular, the agency is

bound by rules concerning the divulging of information, the permissible contents of personal reports, disclosure of the information to the subject, and the registration of any disagreement by the subject including, unlike the Quebec legislation, the duty to inform recipients of the report of the disagreement. Like the Manitoba Personal Investigations Act, this legislation is penal in nature.

6. The Development of a General Right to Privacy

As can be seen from the preceding analysis, the law relating to privacy in Canada may be deficient in a number of respects. In some instances, it fails to extend to situations which individuals regard as requiring protection from intrusion, and in others it provides inadequate protection by reason of certain conditions that compromise the extent and operation of these laws. Nevertheless certain important developments can be noted.

In the common law provinces, we have already seen that British Columbia and Manitoba have enacted legislation specifically making it a tort to violate privacy. On the judicial side, certain common law judgments by the courts have shown considerable responsiveness to privacy problems arising in various areas, such as defamation and confidentiality. On the other hand there is as yet no specific common law tort of invasion of privacy. Such recognition as has been accorded to privacy in tort law by the courts has, therefore, been sporadic and strictly confined to remedies sought for invasions definable in law in other areas.

It appears likely that in the legal interplay between legislatures and courts, protection of privacy in the common law provinces will increase in the face of challenges to personal privacy and related values posed by the development of increasingly efficient information systems containing personal data. It is by no means clear, however, that a general tort of privacy will be developed by the courts, although statutes such as those enacted in British Columbia and Manitoba may contribute to such a development.

In Quebec, the fault-oriented delictual régime based on Article 1053 of the Civil Code has also permitted progress. Indeed, some have argued that the case of *Robbins v. the C.B.C.*,[32] decided on the basis of Article 1053, has established that there is a right to privacy in Quebec. However, it is well to note that this is thus far the only case on the matter. Furthermore, it has been suggested in French

doctrine, which might be relevant to Quebec, that such a right could be seen as a *droit de personnalité* under the civil law.

The federal Parliament may also be able to protect privacy by use of its criminal law power. It has not done so in a general way, but the Protection of Privacy Bill is one step that demonstrates responsiveness in the area.

Whether viewed optimistically or pessimistically, it is clear that case law in Canada contains no comprehensive concept of privacy to inform court decisions or legislative enactments. Thus far, Canadian law provides insight, if at all, only into various negative conceptions of privacy in terms of particular "pinpricks" or invasions of it. These are merely seeds, legislatively and judicially scattered in different parts of the field, whose prospects for sprouting into a coherent notion of privacy are by no means certain.

The Task Force is of the view that a coherent claim to privacy of information is developing and that its definition and elaboration in law would be beneficial. This could serve to inform future court decisions, lead to more effective legislation and generally produce a better understanding of the nature of the issues at stake regarding privacy.

On a conceptual plane, it is possible to argue that every fact about an individual in our society is directly related to his personality and, in consequence, that he has a basic and continuing interest in these facts not being disseminated to others without his knowledge and consent. Society may intrude in a variety of ways for a variety of reasons to require that individuals disclose certain facts, but in doing so it should seek to give due weight to his basic claim to privacy.

There may be a certain "core" of privacy which (although its boundaries may be legitimately varied by judicial and legislative action in response to other social claims) must not lightly be invaded lest an individual's personality be violated. The same consideration applies whether or not the individual concerned is aware of the invasions or not. Once this claim to a core is recognized, consideration could be given to its legal boundaries. This would require a balancing of individual and other interests in society. Consideration would have to be given to whether certain types of information have a special claim to protection (quite likely a very small category including, perhaps, religion, ethnic origin, political beliefs and sexual behaviour). Though the advantages resulting from databanks would have to be given due weight, the terms and conditions governing both the disclosure and the further

dissemination of the various categories of information would also require examination. Thus a *right* to informational privacy would be recognized in principle by society and legally sanctioned. The limits of the right would be then a matter for determination by legislation and through the judicial process, and ultimately through socio-political discourse.

Philosophically, the notion of a core of privacy represents a continuation of our liberal socio-political tradition which has already recognized and characterized other rights flowing from personality, such as freedom of speech, freedom of worship, freedom of assembly. But it may also be looked upon as a culminating right in that it relieves the individual of having to assert particular claims to be left free to engage in particular activities, such as speech, worship and assembly. In asserting a right of privacy, he may simply demand the right, as Warren and Brandeis put it, "to be let alone" to pursue whatever his fancy dictates within the boundaries of the law. Viewed in this light the right would extend the range of rights already recognized to its logical conclusion by encompassing the freedoms already mentioned as well as other rights flowing from personality.

Juridically, legal development of the right might proceed through the general development of case law or by the enactment of appropriate statutes in the various jurisdictions. In this connection, the British Columbia and Manitoba statutes are significant, although they do not go far in defining the right or weighing it against other social demands. The work of the Commissioners on Uniformity of Legislation and of various study groups in the common law provinces would seem to indicate that the two statutes might be the precursors of additional and more extensive enactments.

In Quebec, the Office of Revision of the Civil Code has already proposed the adoption of a bill of rights for Quebec which it regards as confirming an existing legal right to privacy rather than enacting new law. In proposing the bill, the Office stated that its proposal was founded on Article 12 of the Universal Declaration of Human Rights which "has begun to be applied in Quebec jurisprudence." Article 12 proclaims that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

At the federal level, the Canadian Bill of Rights has been

regarded by some as the appropriate statute in which to include a right to privacy. This would have to be very carefully assessed, however, in the light of a variety of factors including the applicability and status of such a federally-created right in Canada.

In any case, whether or not appropriate privacy statutes are enacted and however carefully they define a concept or concepts or privacy, it will still be largely for the courts to determine whether claims to privacy in particular cases are to be accepted and, in making such adjudication, to define authoritatively the contours of the privacy "core" in the light of other social claims. This could lead to a more coherent law flowing from a direct approach to the problem.

Beyond this, a coherent notion of a right to privacy could serve to sensitize judges, legislators and private and public bureaucracies to claims to informational privacy on the part of individuals and in clarifying what is in fact being claimed. It would, even as a principle recognized at the level of serious social and political discourse, provide individuals with a basis from which to work towards enshrining the right to privacy in law.

7. The Adequacy of the Response

Even if a right to privacy was established in Canadian law, to what extent, in the light of the empirical findings of the Task Force, can a court-oriented response to the actual and potential problems of privacy raised by information systems be adequate? In the Task Force's view, the courts alone can provide only partial solutions.

One of the difficulties is that, as our empirical studies show, privacy is only one of the issues raised by the increased utilization of computerized data systems. Beyond privacy, there is the need to prevent harmful information from being disseminated, the right of access to information, questions of accuracy, and the like. There is also, the individual's need in the face of vast organizational informations systems to be included in the calculus of any governmental response. To attempt to meet these and other interests or claims raised by the rapid development of automated information systems on the basis of judicial approach is simply impractical, if not impossible.

Another major reason why a court-oriented approach to privacy may be inadequate lies in the nature of the judicial process. Reliance on the courts alone, either through the development of

common law principles or through judicial interpretation of legislative provisions, has a number of drawbacks. Litigation can be costly and time-consuming; principles are developed slowly and on a case-by-case basis even where statute law has been enacted; those who are in a position to avail themselves of the courts may not be representative of the social groups most frequently suffering invasions of privacy; courts may lack the necessary expertise to deal with rapidly changing computer technology; the use of the courts is likely to be principally limited to situations involving substantial pecuniary considerations, whereas equally serious invasions of privacy not involving direct monetary loss might never be brought before the courts; and courts are generally oriented to the redress of specific past wrongs. Invasions of privacy may in fact be constant, nagging and often minor, and may frequently occur without the knowledge of the person concerned. There is a need therefore for the continual surveillance of information systems with a view to preventing these violations, to supplement the court-oriented process of redressing *post facto* wrongs.

Ultimately what seems to be required, in addition to the remedies that the courts can provide, is a more flexible approach taking account of the requirements of the most effective development and utilization of computers for their designed objectives. Such an approach would be related more to the administrative or regulatory process than the legal-judicial and it is to a discussion of this that the Report now turns.

[1] Warren and Brandeis, *The Right to Privacy* (1890), 4 Harv. L.R. 193.

[2] Roscoe Pound, *Interests of Personality* (1915), 28 Harv. L.R. 343.

[3] S.O. 1965, c. 102; R.S.O. 1970, c. 362.

[4] Radio Act, R.S.C. 1970, c. R-1.

[5] An Act to Incorporate the Bell Telephone Company of Canada, 1880, c. 67, s. 25.

[6] Protection of Privacy Bill C-6.

[7] Criminal Code, R.S.C. 1970, c-34.

[8] Privacy Act, S.B.C., 1968, c. 39; Privacy Act, S.M. 1970, c. 74. And see *Davis v. McArthur* (1970), 72 W.W.R. 69, 10 D.L.R. (3d) 250; appealed 1970, 17 D.L.R. (3d) 760.

[9] *Robbins v. Canadian Broadcasting Corporation* (1958), 12 D.L.R. (2d) 35.

[10] *Green v. Minnes* (1891), 22 Ont. R. 177.

[11] *Pollard v. Photographic Co.* (1888), 40 Ch. D. 345.

[12] *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.* (1963), 3 All E.R. 413n.

[13] *Ibid.*, p. 414.

[14] *Argyll v. Argyll* (1965), 1 All E.R. 611.

[15] *Ibid.*, p. 625.

[16] *Ibid.*, p. 619.

[17] Statistics Act, R.S.C. 1970, c. S-16.

[18] Income Tax Act, S.C. 1970-71, c. 63, s. 241.

[19] [1897] 2 Q.B. 57.

[20] E.g., *Hedley-Byrne v. Heller* (1964), A.C. 465; *Minister of Housing and Local Government v. Sharp* (1970) 1 All E.R. 1009 (C.A.); *Dutton v. Bognor Regis U. D. C.* (1972) 2 W.L.R. 299 (C.A.).

[21] [1919] 2 K.B. 316.

[22] *Re K. C. Irving Ltd. v. The Queen*, (1971) 4 C.P.R. (2d) 120.

[23] *Williams v. Settle* (1960), 2 All E.R. 806.

[24] *Ibid.*, p. 812.

[25] S.B.C. 1968, c. 39.

[26] *Davis v. McArthur* (see n. 8 above).

[27] S.M. 1970, c. 74, amended S.M. 1971, c. 82.

[28] Manitoba Personal Investigations Act, S.M. 1971, c. 23.

[29] Consumer Protection Act, S.Q. 1971, c. 74.

[30] Public Protector Act, S.Q. 1968, c. 11.

[31] S. Sask. 1972, c. 23.

[32] (1958), 12 D.L.R. (2d) 35.

Chapter 12
Regulatory Remedies

1. Background

A variety of proposals has been suggested for regulating information systems in order to protect individual privacy and the related values that may be threatened. Certain proposals were made directly to the Task Force[1], while others have appeared either in the general literature on the subject or in the reports of groups working on related problems in other countries. These proposals are regulatory in that they focus directly on databank activities; they seek to prohibit certain practices considered intrusive upon privacy and related values, and to facilitate the access of individuals to their personal files, taking due account of the operational requirements of databanks. With the exception of self-regulation by the databank industry, these proposals envisage more or less detailed rules set forth in law and regulations, and implemented under the surveillance of some type of administrative mechanism, and with recourse in law to the courts.

Almost every authority on the subject – most recently the report of the Younger Committee on Privacy in Britain and Arthur Miller in his 1971 book, *Assault on Privacy* – has argued the case

for some form of regulation and, at the very least, for continuing surveillance of the operations of databanks to the extent that they may impinge upon privacy and related values.[2] Self-regulation has also received considerable attention in a major study being conducted by the British Computer Society.

The purpose of this chapter, then, is to describe and analyze the various proposals that seek to regulate databanks and data practices in the interest of individual rights. A number of these proposals have already been embodied in provincial statutes, notably the Consumer Protection Act in Quebec, the Personal Investigations Act in Manitoba, and the Credit Reporting Agencies Act in Saskatchewan. Proposals will also be examined that have been advanced, and in some cases enacted, in other countries as the means by which government could respond to the threats posed by information systems and practices.

In earlier chapters, privacy in the information context was described as a claim or right to a "core" of privacy. In practice, this aspect of personal privacy is inadequately protected. While privacy claims brought before the courts have been fitted into existing remedies, the problem that remains is the lack of a comprehensive remedy for invasions of privacy. There are few laws regulating what personal information may be gathered and compiled by operators of information systems, who may or may not amass personal information and thereby build dossiers on individuals, or who may be given access to them. Regulation of information practices may provide the means by which privacy and related individual interests can be protected.

In discussing the various regulatory proposals, it is important to keep fully in view the fact that they purport to regulate the practices of information systems on which many sectors of society increasingly depend. These systems organize information in a manner which will process and "output" facts to produce knowledge so that appropriate decisions can be made, such as to determine whether there is space for a passenger on a particular flight, on which clients are behind in their payments or who is eligible for baby bonus cheques or unemployment insurance. In short, information systems allow businesses, governments, and other institutions to attend to their needs and to satisfy the expectations of society in an efficient manner. This last is an important point; individuals and groups in society are continually making new and increased demands which can be met effectively only by efficiently-run organizations which in turn must acquire and make use of information about these "client" individuals or groups. Any

regulation of databank operations accordingly must recognize the legitimate interest of public institutions and private corporations in obtaining, processing, and using information in order to do their work properly and fulfil their social responsibilities. Regulation, to be effective, would thus have to protect individuals without unnecessarily restricting the effective operation of legitimate information systems.

2. The Objects of Regulation

In Chapter 10, questions of privacy and related values raised by the information process were classified into five categories of issues, namely: data gathering, file content, data storage and handling, data dissemination and access. The possible regulatory responses to these issues are classified in the same way.

a. Data Gathering

The manner and methods adopted by organizations in collecting data may be unnecessarily intrusive of personal privacy, or may produce other harmful consequences. Some of the proposals for remedying these situations attempt to place some limitation on data-collection methods, while others attempt to restrict the information collected to the purpose it is intended to serve.

Surreptitious listening and watching devices have been identified as an especially harmful method of data collection. Parliament, through its examination of wiretapping legislation, is already considering steps to outlaw the use of such devices in private investigations (except for purposes of law enforcement and state security), and also to make possession of them a crime.

Beyond these measures it has been proposed that the storage in databanks of information that has been surreptitiously gathered by electronic or mechanical devices should be prohibited. This proposal clearly would discourage databank personnel from gathering data surreptitiously. At the same time, as with the proposed wiretapping legislation, certain areas such as law enforcement might be exempted. Most investigatory information about criminals and suspects is accumulated by indirect means. Data such as *modus operandi,* known associates, and personal whereabouts are essential for police investigations of crimes, and their curtailment could seriously impede efficient law enforcement.

In general, it has been suggested that there ought to be guidelines regarding the qualification of data collectors, how they ought

to conduct themselves, and the methods that they should or should not employ.

It has further been proposed that data gathering be limited to information that is clearly relevant to the purpose for which it was solicited. This proposal, which has been described as "limiting the direct enquiry", would help to prevent the collection of unnecessary data and so reduce the opportunities for inappropriate use.

There are, however, a number of difficulties in limiting the direct inquiry. One is that individuals are often in a poor position to dispute the relevance of particular information demanded of them, since giving the information is a necessary condition for receiving a benefit, whether it is one to which the individual is legally entitled (such as welfare) or is part of a commercial transaction (credit). Another difficulty is that many people are conditioned to believe that they must give information when asked to although there is a growing tendency, especially on the part of groups frequently the subject of research (e.g., native peoples, university students) and of government enquiries (e.g., business firms), to ask why the information is sought. Indeed, in one recent British Columbia case a Vancouver mother's refusal to disclose to welfare authorities the identity of her illegitimate child's father was upheld on the grounds that the information was not relevant. A policy of limiting the direct enquiry could strengthen this tendency to question the collection of unnecessary and irrelevant data.

Another difficulty is the highly subjective nature of the alleged relevance of any particular item of information in a particular context. This is a problem for both data gatherers and data subjects and might give rise to many confrontations in the course of data gathering. Guidelines might be of some assistance but could only cover a limited number of situations. Large institutional collectors of data also fear that this type of approach could leave large gaps in information to the detriment of informed decision-making.

Beyond limiting the enquiry, one proposal suggests that a blanket prohibition be imposed on the collection of certain types of data. Exceptions would be made only where they were dictated by an overwhelming and statutorily expressed social interest, and then only according to legally-prescribed procedures designed to prevent misuse. While the lists of proscribed data vary (and perhaps one of the drawbacks of this approach is that agreement would be virtually unobtainable), political and religious views and sexual behaviour are usually included. Great care would have to be taken not to inhibit unduly or censor the flow of information and knowledge in society, especially since people who would not object

to divulging certain information to some enquirers, such as pollsters or academics, might object to disclosing the same information to government or a private company.

b. The Contents of Files

Information, no matter how relevant when first collected, may become obsolete over a period of time. Examples include past criminal history, past financial misfortunes, past physical illness, and the misdemeanours of adolescence. One of the most persistent fears of the impact of computers upon the information process is that their very efficiency will ensure that no errors or misfortunes will ever be forgotten, nor in effect ever forgiven.

Although all are not required to do so by law, a number of information systems provide explicitly for the expunging of obsolete information in personal files. It is not uncommon for employer-employee contracts to contain provisions in this respect. General guidelines regarding expunging of obsolete information have been provided, in which the precise time-limits vary according to the nature of the information and the type of databank.

Accuracy raises even more fears than relevance. When issues such as credit, insurance, or employment are at stake, an individual can be severely harmed by inaccurate information. Tests of accuracy are hardest to define for information which may be literally true but inaccurate in context. An example would be the recording of an unpaid debt without a parallel notation of the legitimate reasons for its non-payment. Suggestions have been made that individuals should be permitted to clarify such details by inserting their own account into the record, and this right has been enacted in Quebec, Manitoba and Saskatchewan.

Accuracy is also linked to notions of the currency of data. Out-of-date files may be accurate in their specific content but inaccurate in the light of subsequent events. Thus if a past debt is paid but this fact is not recorded in the file for several months, the file will remain false until it is updated. Since the responsibility for ensuring the accuracy of files rests with the databank operator, it has been suggested that he be required to update and review files periodically.

c. Data Storage and Handling

In terms of storage, privacy is largely a function of "confidentiality", which in turn is a function of system security. The greater the security in which data is held, the greater the degree of protection of privacy provided. Security is not, though, synonymous with privacy. The most secure systems, such as those of police and intelligence agencies, may be the most intrusive of privacy. At the same time, an insecure system adds this threat to privacy to any others that the system may present.

In Chapter 9, the Task Force examined the general state of security of information systems in Canada and analyzed some ways it might be enhanced. The level of security necessary for a particular system is related to the sensitivity of the information it contains and the value of that information to others who might profit from access to it. Financial information tends to be both sensitive and valuable. Medical information, however, often would appear to be valuable only to the individual concerned.

Apart from the sensitivity of information, adequate data security varies among systems depending on their size, their technical characteristics, the value of the data stored in them, and the amount of money available to pay for security. Since the purpose of all security arrangements is to limit access to a system to authorized persons, and since computerized systems are more readily susceptible to protective techniques, automation should provide an opportunity for the establishment of general minimum standards. The principal object of setting security levels would be to make the cost of intrusion – in monetary and other terms – higher than the value of the information obtained.

A key factor in any security system, often overlooked in the rush of attention to sophisticated computer-based passwords and locks, and to encoding techniques for the long-distance transmission of data, is that no security system is stronger than its weakest link. A loquatious enumerator can do more damage than a faulty password. Similarly, the empirical studies turned up the case of highly confidential data contained on a tape being transported in a taxi unaccompanied by any official.

The Task Force has taken note of various proposals that personnel engaged in the processing of personal information should be security cleared and bonded. While security clearances are normal in certain areas of government and industry, the levels of clearance required vary with the sensitivity of the information

involved. It might be difficult to establish general standards. Bonding is normally used as a supplementary measure of indemnification against civil liability and for this reason may be of limited utility.

d. Data Dissemination

The dissemination of personal data about identifiable individuals represents the greatest threat to personal privacy. Information collected from an individual with his knowledge, for purposes of which he approves, can be made available to others without his knowledge and may then be used by them for purposes of which he neither approves nor is aware. This is the point at which an individual can be said most truly to lose control over information about him, at which his fears about "having no place to hide" from his past – immediate or ancient – become most urgent, and at which his privacy becomes most vulnerable.

A range of protective remedies has been proposed. One would impose a blanket restriction on any exchange of information between databanks. A less extreme and more feasible proposition would restrict exchange to recipients who can prove a "need to know", or who are connected to the primary purpose for which the information was collected in the first place. The information disseminated could also be limited to what was directly relevant to the "need". Guidelines to establish the conditions of such permissible exchanges would have to be established.

Another range of proposals concerns the relationship between the subject individual and the databank. Approval by the individual of all proposed data exchanges might be required, or alternatively, since this might entail heavy operating costs, his approval might be required only where information about him is to be used for purposes other than those for which it was originally intended. A related suggestion is that the individual might approve a range of intended exchanges with other databanks at the time the information was collected. A less rigid approach would require the databank to inform the individual of all exchanges, or to furnish a list on demand, and to provide an opportunity for the individual, when he sees fit, to contest a particular exchange in the light of the stated objectives of the databank.

Consent raises a number of complex issues. For one thing, there would probably be objections to an approach requiring advance consultation with an individual in every case where information about him is to be disclosed to others. In another sense,

consent may sometimes be difficult to determine. For example, personal information might be disseminated by a welfare agency, ostensibly for an individual's benefit; he would probably not try to prevent this, but it is questionable whether the consent really would have been freely given. In certain cases, information may have been gathered for a stated purpose, but its uses for other purposes can be of significant benefit to others and to society at large, for example in law enforcement, particularly where state security is involved. Some would suggest that any consent requirement be waived in these cases. They would, however, still want to safeguard privacy, and it has been suggested that law-enforcement authorities seeking access to stored data might be required to obtain search warrants under roughly the conditions specified in the Criminal Code. Certain prohibitions against dissemination already exist, of course, such as those applying to doctors and lawyers, or to the use of tax records or census data[3].

Controls over the dissemination of stored data cannot all be subsumed under a single formula that would apply to every case. There is a danger that over-zealous controls would prevent information systems from functioning effectively, or prevent individuals from having access to information which should ordinarily be made public. Any controls should aim to restrict dissemination to cases of clear need and, whenever possible, to those where the data subject has given his consent.

e. Personal Access to Personal Records

A recurring theme in this Report has been that it is the privacy of *individuals* that may be invaded, while the invasion is done by *institutions,* that is the operators of databanks. The imbalance between the two is evident. This applies at every stage of the process. The individual has disclosed information about himself in order to obtain a benefit; or the information is collected without his knowledge. The databank operator often unilaterally determines the levels of security he considers necessary and, outside a limited range of exceptions, he may also unilaterally decide whether the information should be disseminated to third parties.

This imbalance in power between the subject of information and its possessor is a key reason for many of the regulatory proposals advanced. Yet no matter how much external assistance may be provided to redress the balance by controlling the activities of databanks, the individual remains the protagonist in the drama. Only an individual can determine whether particular types of

information are of importance to himself or herself and therefore worth the effort required to ensure their accuracy or to restrict their dissemination. At present an individual has few mechanisms – other than a court action, or a complaint to his Member of Parliament or to the press – to control the circulation of information about him. The starting point of this lack of control lies in the fact that individuals have almost no knowledge of what happens to information collected about them, and therefore have few opportunities to dispute the uses to which it is put.

Many authors have recommended that people should have a general right of access to stored data of which they are the subject. Access to credit files is incorporated in the United States Fair Credit Reporting Act of 1971, and in the recommendations of the Younger Committee in Britain.

The right of access, in its basic form, would give an individual the right to know of the existence of any file containing personal information about him and to see it on demand. In most versions, this right includes the right to challenge an entry in the record as to its accuracy, completeness, current validity, and relevance. The Quebec, Manitoba and Saskatchewan Acts give the right to insist that his own views be placed on file, permitting him to elaborate on or to clarify personal details in the record which might be vague or misleading.

Most people are aware, at least in general terms, of the existence and location of most of the important files that concern them (financial, credit, insurance, medical). But they probably do not know of them all, nor do they know when important changes in their files are made. Consequently, the suggestion has been advanced that databank operators should notify the individual concerned when they open a new file on him or make major changes in his existing file.

Widely varying types of notification are possible. People could simply be advised that a file has been created and its purposes, or a complete or partial printout of the file could be sent to the individual (the Younger Committee estimated the costs of doing this at between 8¢ and 9¢ per printout). In addition to either of these approaches, individuals might be advised of all uses made of the file or be able, on demand, to obtain a list of these uses.

In selecting among these approaches, a balance will clearly have to be sought between effectiveness in terms of increased benefits to the individual and the increased costs to databank operators. While no hard evidence has been collected, it would appear unlikely that most people would be sufficiently concerned to

seek full information, that is printouts and notification of all uses, on all files maintained about them. Yet some will want to, and would presumably exercise such rights. A satisfactory approach might therefore be to provide individuals with an on-demand right to see a complete version of the file kept by major information systems and to learn of all the uses to which it has been put; this would avoid sending large amounts of unwanted information to individuals through the mails.

Certain practical difficulties in the way of a general right of access and notification on demand must be considered. Some files, such as those of credit bureaux, are maintained in the form of coded alpha-numeric symbols, so that provision would have to be made for a full explanation to the individual requesting access. The value of access can be reduced if databank operators are free to set prohibitive rates for the exercise of this right, as apparently occurred (fees as high as $25 in some instances) immediately following passage of the United States Fair Credit Reporting Act. It is also alleged that some databank operators have used the occasion of visits as an opportunity to gather additional information about the individual.

Even if a general right of access is accepted as desirable, it is clear that important exceptions would have to be made. Medical records, particularly those of psychiatric patients, may well contain information that it would be inadvisable for a patient to see. The records of intelligence agencies represent a clear need for an exemption. Law-enforcement agencies could claim similar exemption, although partial access might be provided. The contents of basic police files can be divided into criminal history and investigatory data. It has been suggested that access might be provided for that part of the file containing a history of criminal acts, including previous arrests, convictions, sentences, all of which are objective and form part of the "public record". Access to criminal history files is provided by the United States Project SEARCH, an interstate police computerized information system. Access to investigatory data, covering details such as *modus operandi,* known associates, and personal whereabouts would be inappropriate.

It has been argued that most people would rarely avail themselves of their right of access, and that databank operators confronted by damage suits arising from false information might argue that failure to exercise the right of access implies acceptance of the data contained in the file. A contrary view is that the existence of a right of access, however little exercised, would provide a powerful incentive for databank operators to upgrade

the accuracy of their files and thus avoid time-consuming, and therefore expensive, disputes with individuals about detailed items of information.

Related to the issue of access is that of informed consent, an issue to which the United States President's Commission on Federal Statistics devoted considerable attention. While the term "informed consent" lacks precise definition, it implies that individuals should be fully informed of the reasons for which information is being sought and the uses to which it will be put.

3. The Subjects of Regulation

As mentioned earlier, the term "databanks" is used as a convenient shorthand for various types of information systems that are not in fact a homogeneous and well-defined class. Although a system of, say, medical records bears certain physical and operational similarities to a system of financial records, the two will be wholly distinct in their contents, style of operation, and objectives. The purpose of regulation clearly is not to control databanks as such but rather to regulate the activities of information systems containing personal data sensitive enough to cause harm to individuals if misused. Thus the degree of regulation which might be appropriate to a databank containing highly sensitive information, such as that of a credit reporting agency, would be quite inappropriate for a databank containing information available to the public, such as that in a municipal registry of property tax assessments.

Despite the glamorous aura of the term, a databank means no more than a store of information from which particular items can be extracted at will. Strictly speaking, for example, a housewife's collection of recipes or a telephone directory are databanks. Much attention has been given by the Organization for Economic Co-operation and Development (O.E.C.D.) to the development of a precise operational definition of a personal databank. That preferred by the Task Force was developed by the Manitoba Law Reform Commission:

> "An information storage operation which can supply personal information about specific individuals, identifiable by name or by means through which the name may be readily obtained."

This definition includes manual as well as automated systems; it excludes statistical systems except in those instances where, in order to update data, coded individual files are maintained. In one

attempt to limit the number of personal databanks affected, a Private Member's Bill introduced into the British Parliament excluded all systems except those containing "one hundred thousand or more names".

At the beginning of this Report, information systems were divided into three broad types: administrative, statistical, and intelligence. Intelligence systems, for reasons of security, represent a special class and would normally be excluded from any general regulatory process. Administrative systems represent by far the largest class and, for the purposes of rule making, it may be useful to subdivide these into internal (employee) and external (customer, client, subject) classes, and to sub-divide the latter into functional groups such as finance, medical, etc.

Two other approaches which ought to be noted would restrain the scope of regulation by concentrating attention upon actual problem areas. It can be argued that general regulation is inappropriate, and perhaps not feasible given the wide variety of subject types. Regulation could rather be directed towards specific areas, such as that of medical records, as proposed by the Ontario Medical Association. Comparable action in the field of credit has been undertaken by Quebec and Saskatchewan, and has been debated in the Ontario Legislature.

The advantage of this approach is that attention is given to specific areas where it is required. Difficulties include the establishment of widely differing standards, a dispersion of expertise, and the fact that certain relatively small but important areas may never be attended to at all.

Another distinctly more academic approach has been to try to develop some form of "information sensitivity scale", beginning with the most sensitive, such as personal sexual morals, and concluding with the least sensitive, i.e., information already available to the public, such as street address and telephone number. An approach of this type has been made by a team at the University of Oslo as part of a study for the Ministry of Justice. The ineradicable difficulty is that any item of information gains sensitivity and importance only in the context of use. However, while no objective "information sensitivity scale" can be devised, information in a *particular* databank can be graded on the basis of sensitivity, and different rules applied to different grades, as in the distinction between criminal history and investigatory data in police records.

A consideration of more fundamental significance resides in the need to make a sharp and clear distinction between regulation of databanks in respect of privacy and regulation of databanks as

such. Control over databanks insofar as privacy is concerned must not be allowed to proliferate into control over the information itself. The consequences, if this happened, including censorship and information selection, could be far worse than the disease that regulation was intended to cure. The Task Force therefore takes it as axiomatic that if any regulatory model were to be adopted, its responsibilities should be limited strictly to those activities of databanks which relate to privacy.

4. The Mechanisms of Regulation

Most regulatory models comprise a set of rules governing databank practices, to be set forth in statutes, together with an administrative mechanism with some role to play in implementing the rules (although this varies among different proposals). Enforcement of the rules might be left entirely to the ordinary courts or to an administrative mechanism (although the courts would retain the final authority in matters of law arising from the operation of databanks). Three possible mechanisms are an independent regulatory tribunal, a surveillance agency, and a complaint mechanism or Ombudsman. These mechanisms, which are examined below, are not mutually exclusive, and the adoption of a regulatory model embodying elements from all three is quite conceivable.

Operating rules or guidelines could be included in statutes directed at databanks generally, or in statutes regulating particular activities, such as banking, which happen to use databanks. While the regulatory mechanisms outlined below envisage general statutes, the latter alternative is also discussed.

a. Independent Administrative Tribunal

A number of proposals envisage the establishment of an administrative tribunal or regulatory board with responsibility for supervising the practices of databanks as they affect privacy and related values. Within guidelines laid down by a legislature, such a tribunal could regulate databanks in respect of matters such as security standards, data-collection procedures, accuracy and relevance of data, exchange of data with other databanks, provision of opportunities for access by subjects, and notification. Normal practice is for the legislature to set down the objectives of the regulatory body (as for example in the case of the Canadian Radio-Television Commission) and establish fairly broad operating guidelines, but to leave the regulatory body free to make decisions in particular

cases and develop additional regulations in the light of experience. The regulatory body could monitor databank activities and hear individual complaints. The enabling legislation would establish clearly the classes of databank falling within the authority of the statute, and these might then be subject to licensing. The recent report of the Swedish Ministry of Justice[4] proposed a compulsory licensing system, whereby a licence from a Data Inspection Board would be required before personal information in any databank (or register) could be computerized. A licence would be granted "if there is no reason to believe that undue encroachment on privacy will result from the register." To prevent intrusions on privacy, the Board would prescribe conditions governing the collection, handling, and dissemination of data.

The essential advantage of a formal regulatory body lies in its ability to prevent, or at least minimize, the occasions for invasions of privacy by ongoing supervision, rather than by having to react only after the fact. By virtue of its power to issue and revoke licences and to formulate and amend regulations, the board, presumably with sufficient expert advice, would be able to maintain a high degree of flexibility to meet the exigencies created by rapidly changing technology.

The deficiencies of this approach derive from the fact that a formal regulatory board is, even in the best of circumstances, a fairly heavy-handed instrument to deal with a subject as evanescent as personal privacy. A determination of whether privacy has been invaded in a particular instance requires an exercise in subjectivity quite unlike that required to determine, for example, whether a particular television station has fulfilled its Canadian-content requirement. The development, in legal terms, of a privacy "core" concept might prove helpful. Nevertheless, it is likely that a sizable area of discretion would remain, along with the possibility of arbitrary decision-making in this very sensitive and complex area.

b. Surveillance Agency

Throughout this Report, qualified phrases have been used such as "potential invasions", or "circumstances which might lead to invasions". Aside from the caution endemic to authors of all government reports, the fact remains that, while there is evidence of concern among the public, and clear evidence that invasions can take place, no proof of widespread invasions actually occurring has been advanced in this or in any other study of the issue. At the same time there is little reason to be sanguine; we have also noted

the continuing, and seemingly inexorable, advance of information technology.

The Younger Committee, after its two-year study, recommended: "That the Government should legislate to provide itself with machinery for keeping under review the growth in and techniques of gathering personal information and processing it with the help of computers." A somewhat similar proposal was advanced by the United States President's Commission on Federal Statistics.

The functions of such an agency could encompass that of continuing surveillance of the techniques and procedures of data collection, storage, and distribution, with particular attention to technological innovations. It could be empowered to investigate, in respect of privacy and related values, major new planned systems, whether in the private sector such as, for example, the so-called "electronic banking systems", or in the public domain, such as proposals to establish a Single Identifying Number system. The agency could make reports, containing recommendations for consideration by government, on such new systems, and could be empowered to issue regular reports on the state of information privacy, with recommendations where appropriate.

Such an agency would have no enforcement powers, but would derive authority both from publicity accruing to its reports and from the force of its recommendations. If linked to an ombudsman-type function, the agency could also receive complaints from members of the public, investigate these and where necessary, issue reports on its findings. For the agency to operate effectively, registration of all databanks within its jurisdiction would be required, providing the agency with full details (which could in turn be made public) of the nature of the information systems and of information-handling policies.

The agency could play a valuable "radar" role. It would provide a mechanism for the scrutiny, in the public interest, of major new information systems, and it could sensitize both government and the public to potential and actual dangers. Moreover, these benefits would be achieved without the inescapable intrusiveness of a regulatory board.

The outstanding drawback to a surveillance agency is its lack of enforcement powers. While it would be able to draw attention to, for instance, inadequate security standards, it would lack any mechanism to ensure that deficiencies were rectified. The agency would constitute also a source of expertise, at present lacking, by which government could check the extent to which its agencies that

are already regulated, in respect of their information handling activities, were in fact fulfilling the requirements of their statutes.

c. Inquiry and Complaint Mechanism (Ombudsman)

The basic theory of the Ombudsman scheme is familiar to most Canadians. The officer, called the Public Protector in Quebec, now exists in six provinces. His task is to receive complaints from members of the public about their treatment by various government agencies and, through his knowledge of and contacts with the bureaucracy, to attempt to resolve the citizen's problem. While generally he lacks the power to order a department to pursue a given course of conduct, the effectiveness of the Ombudsman lies in the prestige of the incumbent, and in his ability to make specific reports to the legislature.

In the West German state of Hessen, an Ombudsman has been appointed, with the title of Data Commissioner, to supervise the operations of personalized databanks. A subject who feels that the practices of any given information system offend against his sense of personal privacy can lay a complaint with the Data Commissioner. The Commissioner then investigates the allegation and, if it is well founded, takes up the matter with the databank operator. A process of mediation and compromise will usually alleviate the complainant's problem. Databank operators are likely to settle difficulties amicably in most instances, in order to escape possible legal action by the complainant, mention by the Commissioner in his public reports, or, possibly, specific legislative action to prohibit the offending practices.

This Ombudsman model has several points in its favour. The structure is simple, requiring far less expenditure of public funds than other models. The privacy-protection function might be tied to related concerns of a civil-libertarian nature, such as those of the proposed Human Rights Commissioner. Although effectiveness depends in large measure on the personal standing of the incumbent Ombudsman, in most cases his findings and recommendations can be expected to be quite authoritative and to receive immediate attention. Moreover, this model appears to respond directly to the problems encountered by individuals; in this sense at least it offers the most immediate solution to citizens' problems.

Still, the Ombudsman model is not without flaws. Principally, it suffers from an incapacity to look at the field as a whole, because the Ombudsman lacks the competence to make investigations of individual databanks without first receiving a complaint from a

person adversely affected. A secondary drawback might be that an Ombudsman, under normal circumstances, would lack the technical expertise required to consider matters such as security standards. However, the mere existence of such a mechanism might be in itself a strong inducement to databank operators to give greater attention to questions of privacy.

d. Alternative Regulatory Strategies

Most regulatory proposals are formulated in terms of rules and structures. The rules and structures are, however, separable. Databank regulation can be decentralized and implemented without a central regulatory authority. The United States Fair Credit Reporting Act of 1971, for example, specifically requires commercial credit bureaux to allow personal access and to provide notification of the existence of files, but leaves the adjudication function to the courts. By means of existing legislation, the rules discussed earlier could be imposed by governments on institutions maintaining personal information systems that are already subject to government regulation in respect of some or all of their operations. In addition, new laws could be enacted to bring other institutions under the régime of databank rules.

Existing laws that may be useful in this context include those which at present affect private or semi-public institutions, as well as administrative statutes regulating the operations of government organisms themselves. Chartered banks, insurance companies, and certain common carriers and their respective governing statutes fall into the first category insofar as the federal government is concerned. Amendments to the statutes and/or regulations imposing rights of access to stored personal information, obligations of accuracy, and rules to govern data security and dissemination would be one available means of regulating these databanks.

Governments could also make use of existing administrative statutes to impose databank rules on government bodies which handle personal data. The example of the confidentiality provisions in the Income Tax and Statistics Acts could be extended to various social assistance and other statutes. Furthermore, internal administrative records, such as employee files, could be protected under some or all of the various rules discussed above by amendment to the employment acts which govern the rights and duties of provincial and federal civil servants. Initiatives in this respect have already been taken by a number of unions in collective bargaining agreements with employers.

In addition, statutes affecting the rights and duties of semi-public institutions such as hospitals, school boards, and universities could be altered to include regulatory prescriptions for personal data handled by these institutions. The province of Ontario has already started to move in this direction with respect to the records of students.

The major advantage of this type of particular rather than general approach is that it can be directed to specific problem areas. Its major defects include the lack of formal structures for "due process", fair hearing, appeal and so forth, and the danger that privacy protection under administrative law might tend to become somewhat haphazard and uneven.

e. Self-regulation

Broadly speaking there are two types of self-regulation. A group may decide voluntarily to regulate certain aspects of the conduct of its own members. Examples range from the Code of Ethics developed by the Association of Credit Bureaus of Canada to the less formal action taken by automobile manufacturers in respect of car safety – an example where the imminence of government action proved a spur to voluntary self-regulation. The second type concerns professions such as those of law and medicine, where the state enacts legislation requiring that persons who wish to engage in these occupations be licensed or certified, or join a particular association to which it delegates certain rule-making and enforcement powers over all its members.

No matter which type is employed, self-regulation imposes a clear burden upon those to whom it applies: at times they must place the public interest before their own interest in situations where the public has no direct means of expressing its interest. Where self-regulation is purely voluntary the members of the group, such as the Association of Credit Bureaus, have no power other than that of moral suasion to enforce compliance; any member can continue in business even if he is expelled from the group. While voluntary self-regulation has advantages – it can create a moral obligation without establishing bureaucratic structures – its potential appears to be too limited to be relied on as the principal means of protecting privacy.

Self-regulation authorized by the state, either in relation to computer operators (technical personnel involved directly in computer operations) or corporate individuals (databank operators, computer service bureaux) merits more detailed consideration.

When supported by some enforcement powers, self-regulation may be an appropriate means of ensuring high standards and of protecting the public against incompetence. The main difficulty with state-authorized self-regulation, however, is that it may often be used as a means to advance the interests of the profession and to restrict competition. The executive of a professional association is faced with a basic conflict between the interests of the profession and those of the public.

It can be argued that the dependence of professions such as law and medicine on a sound public image to attract clients has resulted in a certain measure of congruence between the self-interest of those professions and the public interest. However, even if this is so (and it is far from universally accepted), it would appear that in the computer industry the self-interest of the occupation might tend to pull in a different direction from that of the public. The clients of those providing computer services are not the persons affected by the collection of data, but rather large corporations and institutions. The implementation of costly and time-consuming measures to protect the privacy of personal data would bring far less evident benefits to the computer industry than they might to the professions.

In addition, many of the factors which have generally led to self-regulation in other industries or the professions appear to be absent in the computer industry, most notably in that members of the industry come from widely varying backgrounds and disciplines. Nevertheless, the British Computer Society has taken an initiative that many other national associations have shown an interest in duplicating, both by establishing computer practitioners as professionals and in developing a code of ethics to guide their conduct.

There are many areas where government activity cannot effectively, and no doubt should not, go. One Study prepared for the Task Force quotes Mr. Justice Douglas of the United States Supreme Court:

> "By and large, government can operate satisfactorily only by prescription. That leaves untouched large areas of conduct and activity; some of it susceptible of government regulation but in fact too minute for satisfactory control; some of it lying beyond the periphery of the law in the realm of ethics and morality. Into these large areas self-government, and self-government alone can effectively reach."

One example of effective reach by means of self-regulation is

provided by the York University Behavioural Research Institute, which has developed a code of ethics to be applied to all research conducted under its auspices. Ethics committees have been instituted or are being considered at a number of other universities. Self-regulation, however developed, can sensitize members of a particular group or industry to social responsibilities that might otherwise have been overlooked or neglected. It can raise the level of public confidence in that industry or group. It can lessen the need for state intervention, an important consideration for some users of personal data, such as social science researchers.

For all these reasons it is clear that any and all moves toward self-regulation in respect of the privacy of the subjects of files should be encouraged. At the same time the balance of evidence indicates that such moves cannot be counted on by themselves to resolve all the problems.

5. Regulation of Government Activities

Among the briefs presented to the Computer/Communications Task Force, to which this Task Force had access, were two from departments of the federal government and two from agencies of provincial governments, which drew attention to the particular responsibility of governments, as the largest collectors, storers, and disseminators of data in the country. The O.E.C.D., which has conducted several studies into the area, concluded:

> "It is Governments that can do the most to help since Governments are the most assiduous collectors, evaluators and transmitters of information and are thereby in the best position to enforce high standards and set good examples."

Specific legal requirements to report personal details are part of the reason for the massive quantities of data collected and stored by government agencies. No equivalent duty exists with respect to the data flow between individuals and institutions in the private sector. Additional masses of data grow out of the exclusive government responsibilities for general law enforcement and state security. Finally a great deal of personal information collected by governments is related directly to the many forms of transfer payments given to qualifying citizens (e.g., pensions, baby bonuses, etc.). These programs, and consequently the information stores

connected with them, are dispersed through many different departments and agencies of government at the federal, provincial and municipal levels; this very dispersal often leads to duplication and to the artificial augmentation of the number of personal files held by different government agencies.

This decentralization is held by some to be an important safeguard for individual privacy. Indeed, it was amid the furor created in the United States by the unsuccessful proposal to establish a centralized comprehensive National Data Bank that the computers-and-privacy debate was launched in 1965.

While decentralization of government information remains the rule, proposals for the regulation of government databanks in the name of personal privacy focus upon the transfer and sharing of data among the different agencies, which is frequently done on a discretionary basis and out of public view. The objective of these proposals, very broadly, is to subject government data-handling to rules and to give it visibility.

It should be noted that to speak of regulating government databanks is not necessarily to imply "self-regulation". This, too, has been proposed and could be accomplished by internal administrative directives which, although they would not have the force of law, would tend to be more obligatory than industrial or professional self-regulation by virtue of the quasi-public character of such directives and the public accountability of government. However, some proposals for the regulation of government databanks envisage a set of rules having the force of law, administered by a separate government organ and enforced either by that body or by the courts. Such proposals would thus encompass many of the same structures and rules which are pertinent to regulation in general. Indeed, the recent British Control of Information Bill, introduced by a Private Member, attempted to regulate all databanks, including those operated by the government.

Nevertheless, there are certain factors peculiar to government that tend to limit the possible regulatory structures applicable to government systems. By the same token, certain other regulatory mechanisms become available for government regulation although they may be inappropriate in the private sector.

The model of an independent administrative tribunal, with its characteristic licensing function, is particularly inappropriate to government systems. The independent tribunal has developed to serve the function of regulating competing financial interests in the light of national economic and social policies. Independence from the political organs of government is safeguarded in order to

permit them to adjudicate individual rights and claims free from partisan political control.

Databank regulation within government is quite a different matter. It involves neither the regulation of commerical activities nor the adjudication of individual claims. The interest of a government databank is not an economic one; neither is that of privacy for individuals. While the two may at times conflict, they do not compete in a *market* sense. The need of the regulatory structure for independence from government is thereby reduced.

Furthermore, it would probably be unacceptable that a government organ be licensed, particularly by an agency independent of it, to carry on a function that is clearly executive in nature.

There are several different possible forms of administrative mechanism for the regulation of government databanks. As an interim measure, the idea of a purely advisory body has been suggested by the President's Commission on Federal Statistics in the United States. This body could work with government agencies in developing privacy and other related safeguards, investigate privacy-intrusive practices, hear complaints, and recommend necessary changes where required. Its principal utility would be in raising public consciousness about systems, personnel, and establishments and about how they affect individuals. Its chief sanction would be public opinion. However, the lack of an enforcement mechanism would be a drawback that might compromise its effectiveness. This deficiency might be remedied, however, by channelling its recommendations to another authority competent to deal directly with the issues.

Some thought has been given to placing the regulatory function within an existing structure instead of creating an entirely new body. In such circumstances, there is an inherent danger in placing the function in a government unit which itself collects and administers personal information in support of its own activities. A conflict of interest could develop which might allow the regulatory body to aggrandize its functions into becoming a "super databank".

The most striking feature within the government environment is the power to control spending. The regulatory function thus could be aligned to those units of government which supervise departmental spending. If, for example, these central units were charged with the responsibility to set and police privacy and confidentiality standards with respect to the databanks and associated data practices of the various government departments, or to approve expenditures only after a separate regulatory agency had

certified the databanks in question, the central agencies could enforce these standards by means of their existing financial control. The chief drawback to this model, however, is its lack of visibility. Members of the public would have no access to the regulatory process and, hence, might be denied a forum for complaints and even an awareness of what is being done to information about them. This defect might be overcome by assigning the adjudicatory function to the courts or by interposing an Ombudsman to investigate complaints.

6. Constitutional Considerations

The discussion in this chapter on the merits of different regulatory proposals has thus far left aside the important question – for Canada – of the constitutional apportionment of regulatory jurisdiction. In the absence of specific legislative proposals, no precise statement of the division of power between Parliament and the provincial legislatures can be given. However, some preliminary orientation can be suggested.

The provinces obviously have wide power to regulate the computer-oriented information process in all its aspects, under such jurisdictional heads as property and civil rights, local works and undertakings, and matters of a merely local or private nature. The provinces cannot, however, legislate regarding matters specifically assigned to Parliament. Thus, while chartered banks are subject to many provincial laws of general application, the provinces cannot regulate their banking operations, including the computerization of data for this purpose. Moreover, provincial legislative power is limited to the province, and matters of interprovincial or international dimension fall to the legislative authority of Parliament.

Parliament, too, has extensive power to legislate in the area. Among its specific powers, those relating to banks and statistics are perhaps the most important. Again, under the criminal law, Parliament could impose certain standards of behaviour on databank operators as well as other persons. Parliament also has substantial power to regulate activities that extend beyond provincial boundaries, such as national telecommunications undertakings, through its jurisdiction over trade and commerce, over works and undertakings extending beyond one province or connecting two or more provinces, or because a particular activity or matter is or has become of such national significance as to fall within the Peace,

Order and Good Government clause. The stage at which an activity ceases to be merely local within the province and becomes sufficiently interwoven with outside activities to bring it within federal power is a complex legal question that can be adequately dealt with only after a careful examination of the particular activity involved, the state of the industry, and the nature and form of the remedy sought. Both levels of government however, enjoy virtually unlimited powers with respect to their own operations. The importance of this point lies in the fact that the largest bases of personal data are stored in government databanks.

7. International Considerations

Canadian information systems containing individual personal data have much in common with similar systems in most other western countries; where Canadian systems are unique is that a significant number of their databanks are located wholly or in part outside Canadian borders and therefore outside the reach of Canadian law – whether the law is concerned with privacy or with other issues.

The findings about "extra-territorial" Canadian data have been presented earlier in the Report.[5] Certain generalities can be stated here: the volume of such data is large and, by all indications, is growing; much of it is sensitive, in that it relates to matters such as the credit-worthiness of Canadians, their medical history, travel arrangements, and financial positions. With rare exceptions, data about Canadians is stored outside the country for reasons of economic efficiency and at present no regulations inhibit this flow of data, or even record it.

The storage of Canadian data abroad raises a number of issues that lay beyond the strict purview of the Task Force. These relate to the loss of business activity, to the potential loss of sovereignty, and to the fact that nationals of other countries may have readier access to data about Canadians than Canadians themselves. A related problem, which is a matter of a potential invasion of culture rather than of privacy, concerns information systems, used by Canadians, which contain data contributed exclusively or preponderantly by non-Canadian sources. The Task Force, however, limited its attention to the privacy aspects of extra-territorially stored information, and particularly to data stored in the United States, which is the repository for the bulk of Canadian data held outside the country.

On the basis of enquiries made by the Task Force to the

operators of 13 major databanks in the United States holding extensive data about Canadians, it appears that this data (except in one instance, and for reasons of operational convenience) is not differentiated from that of any other origin. In some respects, such as the Fair Credit Reporting Act, United States law may be more protective of the rights of people about whom data are stored and disseminated than is Canadian law. There also appears to be some spill-over effect, since Canadian credit reporting agencies, which are usually subsidiaries or affiliates of United States organizations, apply the United States rules as corporate practice in Canada for standardization purposes, even though Canadian law does not require them to do so. Indeed, if Canadian legislation does not keep pace with that of other countries, it would not be too fanciful to conceive of Canada becoming a "data haven", where United States and other foreign firms keep their databanks so as to evade stricter domestic requirements. The question of national "data havens" has received considerable attention in studies by the O.E.C.D.

The principal problem, then, is not one of the privacy of Canadian data subjects being invaded by data about them stored in the United States. It is rather that data processing and communications business may be lost to Canadians as a result of this foreign flow; that data in United States databanks might be peremptorily withheld abroad for a variety of reasons, including security regulations, court injunctions, etc.; that United States laws might change and leave Canadians less well protected; and that, as a sovereign state, Canada feels some national embarrassment and resentment over increasing quantities of often sensitive data about Canadians being stored in a foreign country.

With regard to these problems, at least four proposals have been made for government policy on the storage of data about Canadian persons in foreign – particularly United States – databanks. They merit study beyond the preliminary analysis undertaken by the Task Force.

The first would be to do nothing and rely on United States law for protection, but there might be serious disadvantages in this course. As already suggested, United States law might change, leaving inadequate safeguards. More generally, it is clearly inadvisable to rely upon foreign laws – over which Canada has no control – to implement Canadian policy or standards.

A second option would be to permit the continuation of the existing trans-border flow and storage but to require companies in Canada storing data in foreign databanks to register with the

government or a registration authority. Under this scheme, information required by the registrar would include the name, location, and corporate structure of the databank, and its principal operational characteristics, together with a description of the type of data stored and perhaps of the frequency with which it is accessed. In addition, they might be required to notify the registrar – and possibly the Canadian data subjects – each time data about them was stored abroad. A possible institutional structure for such a body is suggested in the report of the Computer/Communications Task Force, which proposed that, at the federal level, registration be required for all suppliers of data-processing and databank services who use data networks which have regularly-used terminals in more than one province or extend into foreign countries.

This procedure would provide the first detailed picture of the extent and nature of the trans-border flow of digital information. It could be used both as a monitoring device and as a source of knowledge from which to develop specific policy responses, such as, perhaps, the initiation of incentives to encourage the siting of databanks within Canadian borders and to increase the proportion of Canadian-originated material in information systems which serve Canadian social and economic needs. The most serious drawback to this type of scheme, however, is that it would be cumbersome.

A third possibility would go one step further by requiring that a complete set of duplicate files be kept in Canada. This would be an even more cumbersome procedure and an expensive one. Moreover, it might even be counter-productive, for the risk of privacy being invaded would be increased by having data stored and handled in two locations instead of one. On the other hand, it would permit Canadian subjects to verify the factual accuracy of the stored data, provided that opportunities for access were given.

Finally, and most extremely, there is the option of trying to prevent entirely the storage abroad of data about Canadians. This option, however, is undesirable in principle, for it would seriously hamper the flow of information that is essential to international commerce. Practically, it would be nearly impossible to enforce, given the many methods of transportation and communications for transferring information. Variants of this option, which would seek to curtail this flow by means of fiscal or excise regulations governing data, are subject to similar objections.

Beyond domestic legislation, however, and since the United States is the principal country involved in this question for Canada, it has been suggested that consideration be given to the

possibility of a bilateral agreement on the storage of data by nationals of each country on the territory of the other. Such an agreement might provide for a commitment from each country not to withhold access by nationals of the other to data concerning them; it could establish rules governing access to data by third parties, by courts, by information brokers, etc.; and it could provide for rules of verification.

Despite the advantages of this approach, certain difficulties would have to be considered. These relate, *inter alia,* to the different nature of legal development in the matter of privacy in the two countries, to different laws governing the admissibility of evidence in court, to Canada's own constitutional situation, which would have to be fully studied, to possible United States unwillingness to extricate the data question from the broader question of commerce with Canada.

In developing any international policies, the question of computers and privacy will probably have to be regarded as closely related to the total trans-border flow of goods and services.

Apart from bilateral arrangements, it is also suggested that Canada ought seriously to examine the possibility of multi-lateral international arrangements relating to privacy and the international flow of data. It seems clear that this flow should not be prevented or hindered, both on the philosophical ground that the free flow of information among countries is important in itself, and on the practical ground that people find it useful.

In order to safeguard privacy, however, the possibility of an international convention might be examined, which, while it affirmed the desirability of the free flow of information, would embody a set of model rules for the protection of persons about whom data is stored. This could both enhance national standards of privacy protection and encourage the compatibility of relevant legislation in different jurisdictions. These rules might, as in the case of bilateral arrangements though in perhaps a more general way, cover standards of data security, the right of access to one's file, the right of verification, rules governing third-party access, etc. Such a convention would be compatible with Article 12 of the Universal Declaration of Human Rights, which includes a right to privacy. And although Canada has not adhered to it, the International Covenant on Civil and Political Rights of 1966 provides similar protection.

A convention could recognize the international implications of the question of computers and privacy as well as facilitate the free trans-border flow of information. It could also help to counter the

arguments of those who want to restrict the flow on the grounds that Canadians might be subject to less effective protection if data about them were stored abroad.

A large number of countries are currently conducting or planning studies of computers and privacy. France, at a recent meeting of the O.E.C.D., stressed the importance of international compatibility in any domestic privacy legislation. The International Union of Lawyers is conducting a study for the European Council of Ministers which will include draft articles for the protection of personal and industrial privacy. And the International Telecommunications Union is likely to examine the question of privacy insofar as the telecommunications links to databanks are concerned.

The constitutional considerations relating to the implementation of international agreements in this field have not been examined by the Task Force. Whatever the situation, federal-provincial co-operation would certainly be essential.

Finally, since one of the main purposes of international initiatives by Canada in this field would be to secure by international means the rights that Canadians enjoy at home, attention first must be given to clarifying, and to establishing where necessary, these rights in Canadian law.

[1] See Task Force Studies by C. Fabien, K. Katz, J. Sharp and S. Usprich.

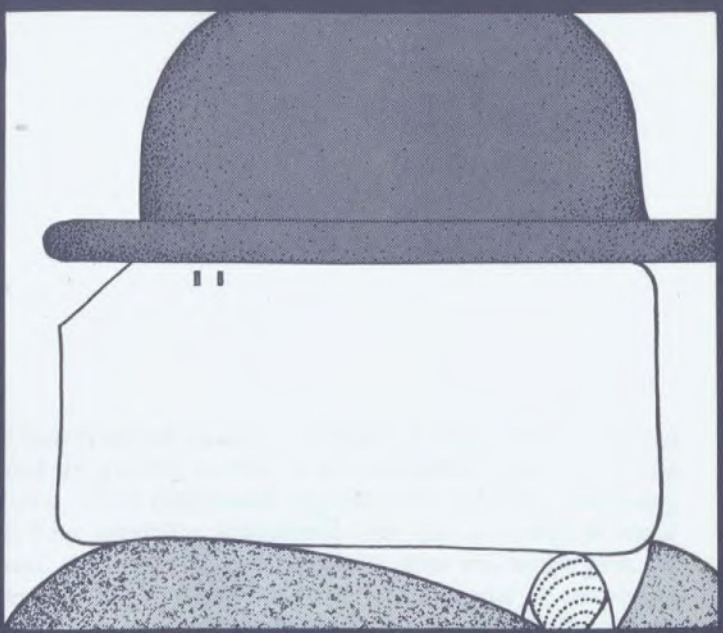
[2] The Report of the National Academy of Sciences in the U.S., which will treat similar considerations, will be published in the fall of 1972.

[3] One subtle distinction raised by the President's Commission on Federal Statistics could be applied to police uses of information that has been gathered and maintained by governments to support benefit programs. They suggest that distribution be restricted to the single purpose of regulating the program itself. Thus, a welfare bureau would not be obliged to transfer information to police which may link an applicant to crime in general, but would supply information if it showed that he had defrauded the welfare system itself.

[4] "Computers and Privacy", summary of report (SOV1972:47) and Draft Data Act submitted by the Commission on Publicity and Secrecy of Official Documents, July 1972.

[5] Subsequent to the empirical studies of the Task Force the press gave considerable attention to a new commercial system, introduced in supermarkets and department stores in the Western provinces, by which shoppers identify themselves by thumb prints when using cheques, which thumb prints are then compared with a computerized databanks in Fort Worth, Texas.

Section VI



Conclusions

Chapter 13
Postscript

The history of our society's evolution in recent generations can be reduced, in graphic terms, to an exponential curve of rising expectations. These heightened expectations, aided by increasing affluence, have created a widespread view that a variety of social claims, such as those to education, employment and health care, are no longer merely privileges but basic requirements of contemporary life. To this list environmental integrity now can be added. Other new, non-material expectations are those to a "right to know" and a "right to privacy".

Whatever the likelihood, or indeed the value, of finding in natural law, written law, or political theory a basis for a "right to privacy", the important fact is that there seems to be an increasing expectation that such a right should be socially and legally recognized. In relation to personal information, this appears to entail the recognition that an individual has a basic and continuing interest in not having information about him communicated to other parties without his knowledge or contrary to his will, except where contending social values justifiably override this interest, and then only under conditions set forth in law.

"A right to know" can be translated into the more colloquial "freedom of information", a goal that at times may conflict with

the search for personal privacy. The conflict between these two goals can scarcely be resolved by resort to abstract formulae but rather must be addressed in the context of particular situations, although the need remains to elaborate a general policy on "freedom of information". This Report has emphasized also the importance of distinguishing clearly between regulation implemented to protect informational privacy and regulation of information as such, an activity that would interfere with the free flow of information and constitute a cure worse than the original ill.

Other considerations, for example the disparity in power between individuals and institutions, stemming in part from the disparity in access to information, arose in the course of the Task Force inquiry. It is evident that the privacy debate encompasses political as well as purely legal issues, the former arising from concern, less about a possible loss of personal privacy than from fear that the possession by institutions of extensive and efficient information systems will enhance their ability to manipulate individuals and to induce conformity. Such concerns cannot be assuaged merely by the adoption of privacy-protective measures; neither can they be ignored. The solutions can only be found in a more even sharing of the power made available by computerized information systems. Information is an explosive subject. So is privacy. So are computers. The boundaries of informed discussion and of responses to the issues must not be drawn too rigidly.

Harm may be done to individuals by the sheer volume of data-gathering, an activity that can become almost an end in itself and, in some instances perhaps, an elegant make-work project. At some future time there will have to come a limit, hopefully before the point when all is known about everybody and everything. An application of cost-effectiveness analysis, or as a last resort of common sense, may advance the date at which this limit is reached. In the shorter term, a case can be made that decision-makers in government, industry, and the universities will have to give serious consideration to the desirability of establishing criteria, based as much perhaps on standards of utility and efficiency as of privacy protection, by which the worth of endless data-gathering exercises can be measured.

Data-collection methods differ as widely as the persons and organizations engaged in them, ranging from policemen to social scientists. Police investigative methods have been the subject of public, as well as of internal, debate; a degree of control will be exercised by court decisions on the admissibility of evidence collected by means such as wiretapping.

The case of social scientists is more complex. Knowledge must be pursued, and in few other areas is our stricture against non-interference with the flow of information more critical. We have noted, however, and by implication praised, the initiative taken by the Behavioural Research Institute of York University in developing a code of ethics to govern its own activities. Such codes remain exceptions rather than the rule. All research institutions and universities might profitably give favourable consideration to implementing similar practices. An alternative approach has been taken by the Russell Sage Foundation in the United States, which imposes a code of ethics as a condition of all research undertaken under its aegis. The Canada Council, the National Research Council, the National Medical Research Council, and other similar funding organizations might give serious attention to the possibility of developing a comparable code of ethics, in close co-operation with institutions such as the Association of Universities and Colleges of Canada and the Social Science Research Council.[1] If implemented, such a scheme could be extended to all research, whether funded by grants or contracts, undertaken on behalf of departments and agencies. At the same time, the possible impediments to research would have to be fully assessed and weighed.

Collection methods are also important to statisticians. A second problem that arises in the context of their work stems from the possibility of residual disclosure extracted from the tables of statistics that are the output of their work. A consultant's study praised the standards and procedures developed by Statistics Canada. Statistics Canada has authority to establish standards to be applied to statistical projects undertaken by all government departments and agencies, but this authority has not yet been exercised extensively. Consideration might be given also to the recommendation made in the recent report of the United States Decennial Census Review Committee that an Advisory Committee should be established as an adjunct to the statistical agency to provide ongoing advice on privacy and related matters.

Among the range of possible responses, that of self-regulation by databank operators would appear to be of limited though by no means of negligible value. The initiative of the British Computer Society in developing a code of ethics may commend itself to the Canadian computer industry; the fact that similar steps have been taken by industries such as advertising and the credit bureaux indicates the scope for useful initiatives.

There are certain limitations to the use of the courts as an instrument for safeguarding privacy in relation to information

systems, particularly since so many of the related issues are more susceptible of administrative than of judicial treatment. However the effectiveness of the courts will grow in proportion to the increase in the volume of litigation on the subject, to the awareness by the courts of the importance of privacy, and to the development and refinement of a general remedy for its protection. An over-all concept of privacy, perhaps along the lines of the notion of a privacy "core" developed in Chapter 11, might serve to guide both general statutory enactments by federal and provincial governments establishing a right of privacy in law, or particular acts governing the activities of specific institutions or industries. A start has already been made in the Acts governing the confidentiality of information collected by Statistics Canada and the Department of National Revenue. Similar action has been announced by Ontario in respect of school records.

For many Canadians, the most important files are those on which decisions are made whether they merit credit, and at what rates of interest. There is no Canadian equivalent to the United States federal Fair Credit Reporting Act, although most provinces are considering or have already implemented measures to regulate, in varying degrees, credit bureaux and credit reporting agencies. Such initiatives are of clear importance; consideration may also need to be given to credit activities which fall beyond the scope of a single province, or which have international ramifications.

Another field that seems to merit particular attention is that of medical and health records – a concern reflected in the briefs submitted to the Task Force, and by the creation, in 1971, of a special Committee on Privacy by the Ontario Medical Association. (It is worth recording that a major study into privacy has been launched recently by the United States Department of Health, Education and Welfare.)

While these initiatives, or already existing statutes, provide a useful source of protection, the response is piecemeal. Government-imposed regulation, exercised by means of a surveillance agency, by an Ombudsman, or by an independent regulatory tribunal, as discussed in Chapter 12, would ensure uniformity and permit flexibility of response.

Although the question of the constitutional jurisdiction over databanks in the private sector has not been explored in depth in this Report, when the time comes to regulate them, it will obviously be highly desirable for federal and provincial authorities to have a consistent and comprehensive approach. Separate actions undertaken by the two orders of government clearly would benefit from

close consultation. The Commissioners on Uniformity of Legislation might constitute a mechanism through which such co-ordination could be achieved.

The old maxim about putting one's own house in order before attempting to scrub those of others commends itself to the Task Force. Governments are by far the largest collectors of data, either directly or indirectly through the medium of grants and contracts for research as well as of on-going administrative programs.

A case can be advanced, therefore, that the federal government, both as a model to others and in order to provide in some degree an operational test-bed, might give serious consideration to the desirability of drawing up rules and creating instruments that could regulate databanks operated by its own agencies and departments insofar as personal privacy is concerned. The protection of privacy and related interests to a large extent represents unfamiliar terrain, and experience rather than theory is likely to prove a more productive way of developing specific rules, and, as important, specific exceptions to those rules. Hence regulation, if it is judged appropriate, should be administered with restraint and, if at all possible, in an environment that allows scope for some experimentation. The fact that the subject of this Report is protection of privacy may cast a shadow over the social and economic benefits that computerized information systems afford; it would be irresponsible to hazard those benefits in order to protect privacy for the sake of show rather than substance.

An instrument for regulating government databanks might take one of several forms: that of an independent regulatory board reporting directly to Parliament, or a regulatory board that reported to a Minister and hence was part of the executive structure; a central department with authority particularly over expenditures, throughout the Public Service, could enforce administrative rules; or some form of Ombudsman, perhaps patterned on the Data Commissioner of the West German state of Hessen, or possibly attached to the proposed Canadian Human Rights Commission. Particular attention might be given to proposals that seek to combine the advantages of visibility (an Ombudsman) with those of day-to-day effectiveness (administrative rules enforced by a central agency).

If the government determines that there is value in implementing this type of regulation, which amounts to a self-imposed restriction upon the operation of its own databanks, an important step will have been taken, we believe, in the development of appropriate protection for the privacy of individuals.

At several stages in this Report we have stressed the fact that despite all the attention given to the subject, neither this study nor others conducted in other countries have concluded that widespread invasions of privacy are actually happening. At the same time we have noted that opportunities for such invasions exist, and expressed the belief that the rapidity of technological progress is likely to broaden rather than restrict the potential for harm to individuals. In Chapter 12, note was taken of the benefit of establishing (as proposed by the Younger Committee in Britain) some form of continuing surveillance agency which would be responsible for monitoring the conduct of databanks within the jurisdiction of the government, for studying technological trends, for considering proposed new systems (an example would be that of a Single Identifying Number), and for issuing reports containing, where appropriate, recommendations for the information of the public and for consideration by the government.

The study of the possible vulnerability to invasions of privacy of data about Canadians stored outside Canadian borders revealed no striking differences that could be attributed to the geographic location of the data. Yet the volume of this type of data, and the sensitivity of much of it, raises questions that relate not so much to possible invasions of privacy as to possible invasions of culture. Business activity may be lost to the country; so also may be that fragile entity, Canadian culture, which is and certainly will be increasingly as sensitive to the content of computerized information systems as it is to the content of broadcast programs.

Critical policy issues are raised by these findings about the extent and content of the trans-border flow of digital information. Any attempt to restrict the flow of information itself would raise serious questions about state control of the flow of information, quite apart from the feasibility of doing so. A first step which may merit serious consideration would be a statutory requirement that Canadian companies and agencies making substantial use of databanks outside the country must register with an appropriate public body. (A possible institutional structure for such a body is suggested by the Computer/Communications Task Force recommendation for the creation of a Register of National Data Networks). This procedure would provide the first detailed picture of the extent and nature of the trans-border flow of digital information. It could be used both as a monitoring device and as a source of knowledge from which to develop specific policy responses, such as the initiation of incentives to encourage the siting of databanks

within Canadian borders and to increase the proportion of Canadian-originated material in information systems which serve Canadian social and economic needs.

Concern has been expressed by some European countries, and the issue has been raised during debates of O.E.C.D., about the possibility that some countries, lacking any regulation of information systems in respect of privacy or of any other value, may come to house "databank havens". As the volume of the trans-border flow of digital information grows, the need for a co-ordination of legislative or other responses at the international level will increase. The United Nations might provide an appropriate forum for consideration of this problem.

In summary, the Task Force concludes:

- "Privacy" is too limited a word to encompass all the concerns created by massive and pervasive information systems. Privacy is used in part as a synonym for political grievances about the use of information systems by institutions to enhance their power to the potential detriment of individuals, and for fears that information systems may be used to manipulate individuals or enforce conformity.
- The principal areas of specific concern about privacy and related values which may be affected in stores of personal information reside in the accuracy or otherwise of the data, in the extent to which the individual concerned has been informed that the information has been gathered and of the uses to which it may be put, in the nature of the controls over the dissemination of data to third parties, in the quality of security techniques, and in the extent to which individuals have a right to inspect and to verify the accuracy of their own files.
- The role of computers is ambivalent. They encourage the collection, storage, and rapid distribution of increasing quantities of data. Yet much of the most sensitive personal information is still stored in manual form; computers, as a function of their efficiency, can be programmed to provide increased protection for privacy.
- Canada faces particular problems. A great deal of personal information about Canadians, much of it highly sensitive, is stored beyond Canadian borders and therefore out of reach of Canadian law. This

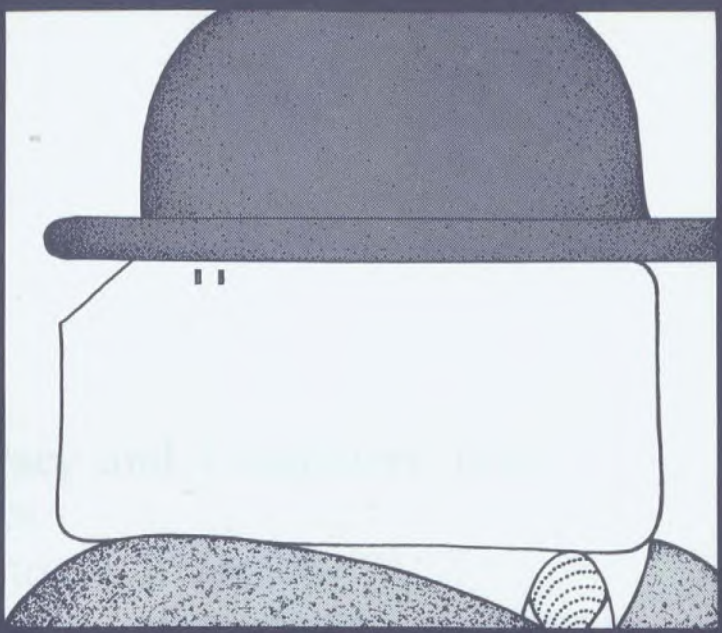
flow of information should be monitored and recorded, and consideration given to encouraging the development of databanks in Canada.

- No single proposal, among the many examined, appears to constitute a comprehensive solution to the problem of invasions of personal privacy. Certain possibilities of particular promise do appear to exist: the utility of some type of surveillance agency combined with an Ombudsman to handle specific complaints by individuals; the important role which could be played by the courts if more claims are brought before them.
- Government, as the principal collector and instigator of the collection of personal information, has a key role to play. Aside from such possible responses as a surveillance agency and an Ombudsman, the government could implement administrative rules, enforced by a central agency, possibly one with control over expenditures, and could also consider developing codes of ethics to govern research conducted with government funds.

Having pondered the issue for a year, the Task Force rejects the proposition that invasions of informational privacy are, in mid-1972, sufficiently widespread to justify description as "a social crisis". Continuing worries exist. Few databanks have been designed and installed with concern for privacy built into the planning process, except for reasons of institutional self-interest. Growth in data-gathering and in the capacity of computer technology shows no signs of abating. If at the same time, as some evidence suggests, the public comes to attach an increasing importance to the preservation of personal privacy, then the measured problem we have described could escalate into one of major proportions. The privacy crisis, unlike the ecology crisis which was predicted but largely ignored until severe damage had been done to the environment, need never happen. Appropriate preventive measures can make certain that in fact it never will.

[1] The Canada Council's *1972 Guide to Applicants for Research Grants* includes the following: "Data collected with Canada Council assistance must be made available within a reasonable time for the use of others *subject to the condition that confidentiality of information and the right to privacy be protected.*"

Appendix



Privacy and Computers Task Force
Terms of Reference

In general, to consider rights, and related values, both present and emergent, appurtenant to the individual and the issues raised by possible invasions of privacy through the collection, storage, processing and use of data contained in automated information and filing systems. And in particular:

a) to examine the types of personal information collected for, stored in, processed by and distributed by automated information systems both governmental and non-governmental, today and in the future;

b) to examine, in terms of their implications for privacy rights and related values, the procedures and mechanisms for the collection, storage, processing and distribution of personal data in automated information systems;

c) to examine and evaluate security procedures and mechanisms employed to prevent unauthorized access to automated information systems;

d) to examine and evaluate possible measures, whether juridical, regulatory, technical or professional, which might ensure observance of privacy rights and values, and to evaluate potential constraints, whether commercial, legal or constitutional, against the application of these measures.

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.

A limited number of copies of the above Studies is available and may be obtained by writing directly to the Department of Communications, 100 Metcalfe Street, Ottawa, or to the Department of Justice, Wellington and Kent Streets, Ottawa. Brief descriptions of the contents of the Studies follow:

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

Abstracts

D.N. Weisstub and C.C. Gotlieb, "The Nature of Privacy"

Privacy as it applies to the individual in relation to fears and realities about the centralization of data, by groups, organizations and governments, and the shifts in the balance of powers which computers bring about. The threat to individual freedoms is looked at in the Canadian context, in an historical and ideological perspective, and in the social, political, psychological, philosophical and legal frameworks.

J.M. Carroll, "Personal Records: Procedures, Practices and Problems"

An empirical analysis of the information systems in Canada, with emphasis upon measures taken to safeguard the privacy of data subjects. Consideration is given to ways of strengthening standards of security and confidentiality in private and governmental information systems. The Study examines, from a privacy perspective, information gathering, storage and dissemination practices in 13 areas of social activity in Canada. Data was gathered by means of a questionnaire, site interviews to selected databank operators and briefs from interested associations and organizations.

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

Describes some existing electronic banking systems and suggests how they might evolve in future. Potential invasions of privacy by these systems and some possible safeguards are also examined.

Technological Review of Computer/Communications.[2]

Projections over the next decade as to developments in computer hardware, software and communications facilities. Consideration is given to directions for changes in systems designed for the storage and retrieval of personalized information about individuals.

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

Examines the methods by which data security can be assured for automated information systems. The Study details the estimate of cost of various security measures, and identifies potential improvements to security systems and procedures.

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

Identifies some of the potential invasions of privacy that might occur through the preparation and use of statistical information. The Study suggests some possible safeguards, together with comments about their possible effectiveness.

J.S. Williams, "Legal Protection of Privacy"

The techniques of enforcement and regulation, through the common law, of an individual's right to privacy. This Study gives an indication of the practical limits to protection and assists in the elucidation of the interests to be protected. It draws attention to areas which could be further developed within the existing legal framework.

J. Boucher, "Vie Privée et Ordinateur dans le Droit de la Province du Québec"

The author examines the extent to which a right of privacy is protected by the Quebec Civil Code and statutes. Although the law does not recognize a right of privacy as such, the laws of contract, property and torts offer various remedies. The author proposes that the law establish privacy as a personal right under the Civil Code.

K. Katz, "Regulation of Federal Data Banks"

Analysis of the different sorts of information systems maintained by the Government of Canada and the relative privacy sensitivity of each. The Study examines various legislative and administrative responses which might be developed to lessen the extent of intrusion upon the individual's core value of privacy. Special emphasis is paid to techniques applicable to data systems maintained by the federal government.

J.M. Sharp, "Regulatory Models"

Examines ways of meeting the threat to privacy of the individual posed by information systems, both computerized and manual. Specific matters considered include appropriate definitions for databanks in Canada; rules for their operation, in the interest of data subjects' privacy; and the feasibility of self-regulation of the data processing industry and its professional staff. Particular attention is paid to possible regulatory models for credit companies.

C. Fabien, "Ordinateur et Vie Privée: Techniques et Contrôle"

The Study examines and analyzes the relative merits of judicial and administrative techniques for the protection of the right of privacy in the context of personal information, including an examination of the technique of self-regulation and of the role of public opinion as a political control mechanism. Of primary interest in this study is the proposal for the establishment of an administrative mechanism in the office of an ombudsman.

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

Sketches the larger theoretical implications of self-regulation and the conclusions they lead to concerning its applicability as a means of controlling the abuse of confidential information in the computer industry.

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

A study of the constitutional aspects of information processing and transmission systems which seeks to identify the respective areas of federal and provincial legislative and regulatory competence under the *British North America Act,* 1867.

C. Dalfen, "International Factors"

A study of the issues created by the existence of databanks containing information about Canadians that are located outside Canadian borders, particularly in the U.S. The Study examines potential problems facing Canada as a consequence of this situation, the effects of foreign laws on "extra-territorial" Canadian data, and possible responses for Canada.

[2] To be published by the Canadian Computer/Communications Task Force.

Questionnaire

As its principal instrument for gathering information, the Task Force sent a questionnaire to 2471 companies, agencies and institutions in Canada. The questionnaire was pre-tested with a sample of 45 organizations. Including 24 pre-test responses, 1268 replies were received.

A copy of the questionnaire, with a breakdown of the replies follows. The breakdown is based on the first 1215 responses received. Later replies did not alter the results significantly. (The symbol, ∅, indicates the number of respondents who failed to answer individual questions.)

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 histroy 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)
Provincal 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-marking	(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 oganization).

$\emptyset$ = 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.).

$\emptyset$ = 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.).

$\emptyset$ = 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.).

$\emptyset$ = 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*).

		$\emptyset$	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 Records (Ø = 27)	(771)	(229)	(86)	(5)	(27)
5. A.2 Subjects or client/customers (Ø = 91)	(387)	(334)	(227)	(10)	(166)
5. A.3 Information recipients (Ø = 122)	(198)	(266)	(172)	(10)	(453)

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 We furnish information (Ø = 45)	(457)	(360)	(59)	(8)	(277)
5. B.2 We obtain information (Ø = 68)	(364)	(421)	(184)	(8)	(249)

5. C. Have you ever seriously considered having portions of your data-processing operations performed in the U.S.?

$\emptyset$ = 39 Yes 151 No 1022

5. D. Under what conditions would you locate files in the U.S.
(Please mark *one* response only). $\emptyset$ = 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*).

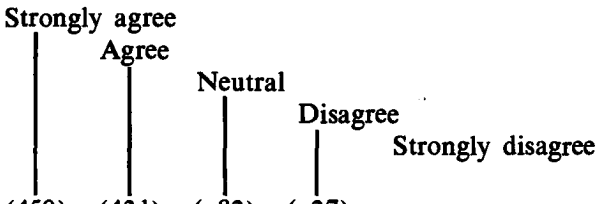
6. A.1
a) We need new and more detailed organizational rules to govern collection and use of personal data. ($\emptyset$) = 39 (242)

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. $\emptyset$ = 43 (229)

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*.)



6. B.1 (450) (431) (82) (27)
To be informed of the existence of such records when started.
$\emptyset$ = 78

6. B.2. (330) (421) (121) (186) (91)
To review on demand the contents of records concerning them.
$\emptyset$ = 66

6. B.3 (422) (478) (97) (88) (52)
To correct, rebut, update, and expunge incorrect or obsolete information concerning them.
$\emptyset$ = 78

6. B.4. (202) (243) (257) (327) (109)
To be furnished periodically with an accounting of the uses made of information concerning them.
$\emptyset$ = 77

6. B.5 (232) (357) (193) (244) (113)
To learn the sources of information concerning them.
$\emptyset$ = 76

6. B.6 (232) (211) (207) (344) (139)
To stop the exchange of information concerning them among information suppliers.
$\emptyset$ = 82

6. C. The following actions regarding data banks containing personally identifiable data are necessary. (Please mark *one* response in *each row*).

Strongly agree | Agree | Neutral | Disagree | Strongly disagree

6. C.1 (422) (419) (161) (95) (25)
Registration as to purpose and contents.
$\emptyset$ = 93

6. C.2 (368) (440) (206) (58) (23)
Standards of hardware and software security.
$\emptyset$ = 120

6. C.3 (435) (461) (143) (49) (24)
Standards concerned with the acquisition and dissemination of information.
$\emptyset$ = 103

6. C.4 (291) (391) (275) (99) (51)
Periodic site inspections.
$\emptyset$ = 108

6. D. The following people and organizations trafficking in personally identifiable information should be licensed and certified. (Please mark *one* response in *each row*).

Strongly agree | Agree | Neutral | Disagree | Strongly disagree

6. D.1 (592) (362) (112) (44) (19)
Databank proprietors
$\emptyset$ = 86

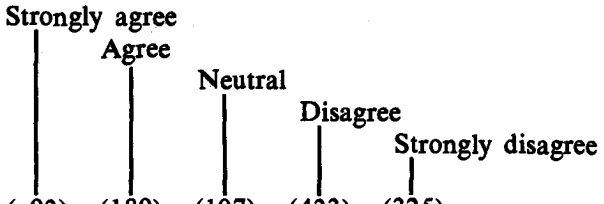
6. D.2 (606) (356) (114) (33) (16)
Information brokers (suppliers)
$\emptyset$ = 90

6. D.3 (479) (346) (188) (86) (35)
Data-processing centres
$\emptyset$ = 89

6. D.4 (376) (255) (265) (176) (52)
Computer programmers
$\emptyset$ = 91

6. D.5 (446) (336) (205) (101) (39)
Data gatherers
$\emptyset$ = 88

6. E. Please mark *one* response in *each row.*



6. E.1 (93) (189) (107) (433) (325)
Records are the exclusive property of the information-system proprietors subjects have no interest in them.
$\emptyset$ = 68

6. E.2 (123) (351) (158) (286) (225)
Information-system proprietors should furnish personal data to law-enforcement officers on demand.
$\emptyset$ = 72

6. E.3 (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 *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	(660)	(106)	(82)	(4)	(279)

General reports are published periodically.
$\emptyset$ = 84

10. A.2	(502)	(267)	(112)	(9)	(235)

Special reports are distributed selectively.
$\emptyset$ = 90

10. A.3	(172)	(600)	(268)	(7)	(112)

Information is furnished in response to specific requests.
$\emptyset$ = 56

10. B. Please indicate the approximate average number of specific requests fulfilled annually. (Please mark only *one* response). $\emptyset$ = 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). $\emptyset$ = 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 (247) (594) (72) (235)
Individuals whose records are maintained in this file.
Ø = 66

11. B.2 (46) (377) (566) (159)
Employees charged with records management.
Ø = 66

11. B.3 (243) (215) (35) (647)
General public.
Ø = 73

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*). ∅ = 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). ∅ = 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?

∅ = 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). ∅ = 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	(451)	(530)	(67)	(34)
	Other information suppliers. $\emptyset$ = 133			
13. A.2	(744)	(288)	(26)	(13)
	Published sources or public records. $\emptyset$ = 144			
13. A.3	(63)	(211)	(474)	(396)
	Individual on whom the record is kept. $\emptyset$ = 78			
13. A.4	(819)	(212)	(33)	(12)
	Information recipients (e.g. merchants). $\emptyset$ = 139			
13. A.5	(745)	(264)	(48)	(28)
	Investigators. $\emptyset$ = 130			

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). $\emptyset$ = 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*). ∅ = 48

	Never used	Sometimes used	Generally used	Always used	Does not apply
13. C.2 Members of subject's family ∅ = 71	(454)	(448)	(98)	(27)	(116)
13. C.3 Subject's neighbours or friends ∅ = 77	(641)	(318)	(22)	(9)	(149)
13. C.4 References nominated by subject ∅ = 73	(220)	(482)	(203)	(102)	(135)
13. C.5 Former employers of subject ∅ = 77	(304)	(413)	(176)	(78)	(167)
13. C.6 Present employer ∅ = 80	(298)	(396)	(126)	(89)	(226)
13. C.7 Medical practitioners and hospitals ∅ = 67	(352)	(310)	(167)	(168)	(151)
13. C.8 Law enforcement agencies ∅ = 72	(574)	(299)	(25)	(18)	(226)

13. C.9 (378) (386) (119) (81) (186)
Educational institutions attended by subject.
$\emptyset$ = 72

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 (93) (95) (211) (420) (317)
Identify himself and present credentials.
$\emptyset$ = 79

13. D.2 (122) (110) (167) (360) (362)
Identify his employer
$\emptyset$ = 94

13. D.3 (116) (107) (154) (372) (372)
Disclose reason for investigation
$\emptyset$ = 94

13. D.4 (162) (87) (96) (250) (524)
Promise to protect informant
$\emptyset$ = 96

13. D.5 (177) (68) (95) 255) (516)
Guarantee the ultimate use of information
$\emptyset$ = 104

13. D.6 (140) (142) (147) (252) (434)
Demonstrate that the subject has consented to the gathering of information about him.
$\emptyset$ = 99

13. D.7 (161) (244) (149) (85) (476)
Confirm facts from at least two independent sources.
$\emptyset$ = 100

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). $\emptyset$ = 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). $\emptyset$ = 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). $\emptyset$ = 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 Employees Ø = 701	(145)	(57)	(62)	(218)	(32)
16. A.2 Clients/Customers Ø = 700	(50)	(79)	(88)	(249)	(49)
16. A.3 Subjects Ø = 73	(122)	59)	(31)	(45)	(235)

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 Employees Ø = 696	(125)	(203)	(121)	(20)	(50)
16. B.2 Clients/Customers Ø = 698	(39)	(236)	(141)	(43)	(58)
16. B.3 Subjects Ø = 724	(103)	(85)	(38)	(14)	(251)

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 have a service bureau or other outside computer facility (205)

19. A. Has conversion of records to computerized form led to detection and correction of actual 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 *one* 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. password, 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 *one* response in *each row*).

	None	Data input only	Information display only	Input and output
20. D.1	(353)	(10)	(5)	(103)

Remote high-speed terminals (e.g. card reader, printer)
Ø = 744

20. D.2 (352) (18) (15) (81)
Remote keyboard terminals (e.g. teleprinters, video displays)
Ø = 749

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 record?

Ø = 792 Yes (11) No (69)
Does not apply (343)

26. Are additional uses 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.

Briefs

Briefs were requested from 187 Canadian industrial and professional associations. The following letter of request was sent to the associations:

April 26, 1971

The maintenance of privacy and the protection of individuals' rights generally are of continuing concern to governments and in particular this concern now is focussing on the special problems posed by the development of computerized information systems.

Studies of various kinds are underway in other countries. In Canada our study commenced with a conference titled: "Computers: Privacy and Freedom of Information", held last May at Queen's University, as part of the Telecommission inquiry into telecommunications arts, sponsored by the Department of Communications and the Department of Justice of the government of Canada, the Canadian Information Processing Society and Queen's University. An advance copy of the report of this Conference is enclosed.

The next step was the establishment by the Minister of Justice and the Minister of Communications of a Joint Privacy and Computers Task Force to give more detailed and in-depth consideration to some of the issues and problems identified by the Conference. The terms of reference of the Task Force are:

> "In general, to consider rights, and related values, both present and emergent, appurtenant to the individual and the issues raised by possible invasions of privacy through the collection, storage, processing and use of data contained in automated information and filing systems. And in particular:
>
> a) to examine the types of personal information collected for, stored in, processed by and distributed by automated information systems both governmental and non-governmental, today and in the future;
>
> b) to examine, in terms of their implications for privacy

rights and related values, the procedures and mechanisms for the collection, storage, processing and distribution of personal data in automated information systems;

c) to examine and evaluate security procedures and mechanisms employed to prevent unauthorized access to automated information systems;

d) to examine and evaluate possible measures, whether juridical, regulatory, technical or professional, which might ensure observance of privacy rights and values, and to evaluate potential constraints, whether commercial, legal or constitutional, against the application of these measures."

To avoid any misunderstandings, we should explain that this Task Force on Privacy and Computers is separate from, though complementary to, the Computer/Communications Task Force from whom you may be hearing in respect of those matters with which it is directly concerned.

The study undertaken by the Privacy Task Force will be extensive; it will draw upon the widest possible base of information and informed opinion, and will examine manual as well as automated information systems. A questionnaire will be distributed to a large number of companies and institutions which maintain information systems, and a number of intensive site interviews will be undertaken, on a sample basis.

The purpose of this letter is to invite your Association to express your views on the general issues of concern to the Task Force. The nature and form of your response, we quite appreciate, will be governed by the interests of your Association, but we would also hope that you would feel free to offer comments on any aspects of the matter, whether or not it is directly related to the undertakings of your members. Some of the issues raised during studies made into this question in Canada or elsewhere are those of formal statements by data bank operators of their objectives, professional codes of ethics, rights of access by individuals to their files, to challenge the accuracy of the contents, to be informed of the use made of the information contained in the files, as well as the issues of technical standards to ensure data and system security, and of licensing of data banks. The list is not exhaustive. It may, however, help you to focus on some of the important aspects of this broad field; at the same time please feel free to ignore any or all of the subjects, and to comment on the many other considerations that are not listed.

Similarly we would be happy to hear directly from any of your members who may wish to express their views. We realize of course that within any groups there may be substantial differences of thought.

A form indicating an intention to file, or not to file, a brief is enclosed along with a self-addressed envelope. We would be grateful if you would return it as quickly as possible, and that you would submit your brief not later than the end of June.

Sincerely,

Richard J. Gwyn
Director
Socio-Economic Planning Branch
Department of Communications

E.R. Olson
Director
Legal Research and Planning
Department of Justice

Privacy and Computers Task Force,
P.O. Box 8350,
Ottawa, Canada K1G 3H8

SURVEY REPLY

We intend to participate in the survey the Computers and Privacy Task Force and

☐ will submit a brief by June 31st, 1971.

☐ do not intend to submit a brief.

Group d'étude sur l'ordinateur et la vie privée
C.P. 8350
Ottawa, Canada K1G 3H8

CARTE-REPONSE

Nous désirons prendre part à l'enquête du Groupe d'étude sur l'ordinateur et la vie privée:

☐ nous présenterons un mémoire au plus tard le 30 juin 1971.

☐ nous n'avons pas l'intention de présenter un mémoire.

Association name and postal address
Nom et adresse postale de l'association.

Name of association's representative
Nom du représentant de l'association

Title
Titre

Telephone No.
No de téléphone

Postal address
Adresse postale

Briefs to the Privacy & Computers Task Force

Briefs were received from the following organizations:

Canadian Association of Data Processing Service Organizations
Canadian Bankers' Association
Canadian Book Publishers' Council
Canadian Business Equipment Manufacturers Association
Canadian Copyright Institute
Canadian Life Insurance Association
Canadian Manufacturers' Association
Canadian Medical Association
Clarke Institute of Psychiatry
Committee of Presidents of Universities of Ontario
Ontario Medical Association
Retail Council of Canada
Retail Credit Company of Canada Limited
Royal Bank of Canada
Telephone Association of Canada
United Community Fund of Greater Toronto

In addition, the Canadian Computer/Communications Task Force of the Department of Communications received 54 briefs that contained references or statements on the issues of privacy.

Foreign Databanks

The following organizations which operate databanks containing personal information about Canadians provided information about their activities at the request of the Task Force:

American Airlines Inc.
American Express
Carte Blanche
Diners Club Inc.
Hooper Holmes Bureau Inc. – Credit Index
– Casualty Index
ITT Data Processing
Institute of Electrical and Electronics Engineers
McGraw-Hill Data Service
National Data Corp.
Recording and Statistical Corp. – Medical Information Bureau
Retail Credit Corp.
TRW Inc. – Credit Data Corp.

Bibliographies

It is expected that a researcher may wish to consult the various reference materials used by members of the Task Force. While the Task Force accumulated a substantial library of books and articles on the subject, the best, most complete and well organized bibliographies can be found in the following works:

Harrison, Annette
The Problem of Privacy in the Computer Age: An Annotated Bibliography.
Santa Monica: The RAND Corporation, 1970
A two volume up-date of an earlier study, commissioned by the U.S. Government. The most complete bibliography on the subject.

Miller, Arthur R.
Assault on Privacy
Ann Arbor: University of Michigan Press, 1971
Bibliography at pp. 261-269. Est. 200 entries, organized as to class of entry.

United States, House of Representatives, Subcommittee of the Committee on Government Operations, 89th Congress.
The Computer and Invasions of Privacy
Washington: U.S. Government Printing Office, 1966;
New York: Arno Press, 1967.
"Letters, statements, etc., submitted for the record--" at pp. 135-311. Relates primarily to information practices of the U.S. Government as they relate to the privacy of the individual.

Westin, Alan F.
Privacy and Freedom
New York: Atheneum, 1970.
Bibliography at pp. 445-458. About 440 entries, ordered under four topics.

Younger, Rt. Hon. Kenneth (Chairman)
Report of the Committee on Privacy
London: Her Majesty's Stationery Office, July 1972 (Cmnd. 5012)
Appendix C, "Select Bibliography", pp. 223-24.

Parallel Studies

Studies similar to that of the Privacy and Computers Task Force have been or are in progress in a number of other countries. The major ones are:

Denmark

Studies undertaken by the Minister of Justice.

France

The Conseil D'Etat has initiated an internal study. No report issued to date.

Germany

In addition to a study sponsored by the Minister of Justice, a number of states are examining the Data Commissioner scheme implemented by the state of Hessen.

Netherlands

A "State Committee on Privacy," installed by Royal Decree of February 18, 1972, has been established by the government. Publication date not yet announced.

Norway

The Institute of Private Law of the University of Oslo, Norway, has undertaken a study for the Ministry of Justice. Note also the report of the First Oslo Symposium on Databanks and Society.

OECD

The Data Control Panel, a sub-group of the Committee for Science Policy, produced a report, "Digital Information and the Privacy Problem," in March 1971.

Sweden

The Swedish Agency for Administrative Development ("SAFAD") published a report on the general issue of privacy, entitled *Data Och Integritet* ("Data and Integrity") in June 1972. An English-Language abridged version is available, entitled "Computers and Privacy" (20 pp., typescript). P.O. Box 2106, S-103 13 Stockholm.

Switzerland

An internal government working group is examining the issue.

United Kingdom

The Committee on Privacy, under the Chairmanship of the Rt. Hon. Kenneth Younger, published its report on July 12, 1972. A volume of 350 pages, convering all aspects of privacy including those related to the operation of databanks, is available through Her Majesty's Stationery Office (Cmnd. 5012) for $2.00.

The British Computer Society, early in 1972, initiated a study of the issue. Particular attention is being paid to the development of a Code of Ethics.

A study group within the British Civil Service is expected to complete its report in 1972. No decision has been taken on publication.

United States

The Report of the National Academy of Sciences, under the direction of Prof. Alan Westin, is scheduled to be published in the fall of 1972. The study, funded by the Russell Sage Foundation, was commenced early in 1970.

The National Science Foundation, early in 1972, commenced a study under the chairmanship of Prof. Arthur Miller.

The report of the Decennial Census Review Committee, published in July 1971, examined the issues of privacy and confidentiality in relation to Census activities.

A Committee, established by the Department of Health, Education and Welfare, began public hearings in April 1972, and is scheduled to publish a preliminary report by Jan. 1, 1973.

See also proceedings of the Senate Sub-Committee on Constitutional Rights under the chairmanship of Senator Sam Ervin.

Index