TELECOMMISSION

Study 5(b)

Conference Report – Computers: Privacy and Freedom of Information

The Department of Communications

Telecommission Study (5b)

CONFERENCE ON
COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

Queen's University
May 21 - 24, 1970

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: $2.00 Catalogue No. Co41-1/5B

Price subject to change without notice

Information Canada
Ottawa, 1971

This is a Report on the Conference and does not necessarily represent the views of the Department or of the federal Government. No commitment for future action should be inferred from the recommendations of the participants.

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

"COMPUTERS: PRIVACY & FREEDOM OF INFORMATION"

PREFACE

The potential impact of computers upon individuals, their values and their rights, and in particular the relation of computerized information systems to personal privacy has become a matter of world-wide concern - as witnessed by the extended hearings in the United States Congress on a proposed National Data Bank, by resolution 1028 of the twenty-sixth session of the General Assembly of the United Nations on Human Rights and Scientific and Technological Developments, and by studies initiated in the United States, Britain, West Germany, Sweden and Denmark. In order to begin this same process in Canada, four groups undertook early in 1970 to sponsor a conference on this subject:

- the Department of Communications
- the Department of Justice
- the Canadian Information Processing Society
- Queen's University

This report summarizes the proceedings and discussions of that conference which was held at Queen's University, Kingston, Ontario, from May 21-24, 1970.

A conference committee and a program committee were appointed to plan the conference. In recognition of the dual importance of maintaining both privacy and freedom of access to information these committees selected as the title for the conference: "Computers: Privacy and Freedom of Information", and set as objectives:

"a) to discuss, examine and define the issues of personal privacy and right of access in the operation of information systems and data banks,

b) to identify the probable problem areas in the application of computer technology to data collection, storage and retrieval,

c) to suggest guidelines for the protection of privacy and of access to information in tomorrow's technology,

d) to record the informed opinions of a representative group of those concerned with the design, operation and use of computerized information systems and data banks on the issues of privacy and right of access."

Three key intentions governed the planning of the conference:

1) every attempt would be made to have a full range of views represented. This would be achieved by appropriate selection of the topics, the invited speakers and the invited participants;

2) every attempt would be made to go beyond the popular discussion of the theme and come to grips with specific problems and detailed proposals. This would be achieved by:
   - limiting conference attendance to participants who already were involved in the subject or who were likely to have some direct involvement in the near future;

- distributing advance review papers to participants, so that they could come prepared, and with some commonality of background;

- organizing multi-disciplinary workshop sessions among small groups of people, to provide ample opportunity for free discussion;

- ensuring that there would be adequate arrangements with respect to the distribution of materials and the recording of proceedings. These would include distribution of the written texts of speakers, summaries to be made by rapporteurs of the workshops, and a final report to be a coherent expression of the whole conference;

- documenting a number of proposals regarding computers and data banks, and recording measures of agreement or disagreement on these proposals;

3) every attempt would be made to set the theme in a Canadian setting. This would be achieved by:

- ensuring that the background texts included materials on Canadian laws and practices;

- keeping in mind the joint federal and provincial responsibilities in the selection of speakers, discussants and participants;

- providing for both French and English contribu-

tions in written materials, and simultaneous translation, in the discussion.

As recorded in the Introduction, the conference achieved a surprising measure of consensus both on the nature and extent of the problems in respect of privacy created by the rapid development of computerized information systems and on the scope of possible solutions to these problems. The formulation of specific solutions to these problems will depend upon the various studies recommended by the conference; their implementation would then be the responsibility of the governments and other institutions concerned.

The overall report of the conference was written by Mr. Ian Rodger of The Financial Post. In the view of the Program Committee, it faithfully records both the extent of the consensus which was achieved, and the measures of disagreement which were revealed. In addition, our thanks are due to Queen's University for the excellence of the arrangements which played so large a part in assuring the success of the conference.

R. J. Gwyn
Conference Chairman

C. C. Gotlieb
Chairman
Program Committee

INTRODUCTION

The holding of a conference to explore the effects of computer technology on personal privacy and freedom of information was, as Justice Minister John Turner pointed out, "of no small significance - and indeed of some historic value." Mr. Turner added, however:

> "It is not so much a matter of self-congratulation as perhaps for self criticism, for the problems posed to privacy and freedom of information by the new cybernetics of a technetronic age have been with us for some time. Indeed, the generic issue of the right to privacy - or the threatened invasions of privacy - has been part of the intellectual tradition and jurisprudential inquiry in the United States since 1890."

While it is true that Louis Brandeis, later Associate Chief Justice of the United States, co-authored a pioneering article in 1890 on a right to privacy, it was not until the 1960s that the issue really gained momentum, in the United States or elsewhere. To trace the reasons for either the general neglect of a right to privacy in the past or the sudden flowering of interest in it in recent years would be a formidable and perhaps unrewarding task. Like pollution, privacy is a 'problem' that has been thrust upon our consciousness.

The particular event that sparked the current concern about personal privacy and the computer was probably the 1965 proposal of the U.S. Social Science Research Council that the Bureau of the Budget establish a "national data center" to organize the efficient retrieval of information about citizens as a consequence of the government's involvement in the complex areas of poverty, health, urban renewal and education. The proposal was presented to a Congressional sub-committee and led to the now-

famous hearings in 1966 on "Computers and Privacy" under the chairmanship of Rep. Cornelius Gallagher. Public and political reaction to the proposal was immediate, vocal and almost wholly negative.

Since then, a wealth of legal articles, books, studies and legislative proposals has appeared.

In the United States a major study organized by the National Academy of Sciences will complete its inquiry by June 1971, and the Congress continues to struggle with this topic. In Britain, Parliament has established a Select Committee to study this issue. In France, the Conseil d'Etat was assigned the task, early in 1970 of studying juridical problems in the computing field, including the challenges computers pose to individual liberties. Sweden appointed a Royal Commission in 1966 to elaborate legislative proposals concerning the protection of privacy in general against invasion by modern scientific and technical devices. Denmark has a similar study in progress.

In the United States, two major books, Privacy and Freedom, by Alan F. Westin, a Columbia University professor, and The Death of Privacy, by Dr. Jerry Rosenberg appeared in 1967 and 1969 respectively. Professor Westin will shortly publish a second book, as will Professor Arthur Miller of the University of Michigan on privacy.

The Organization for Economic Cooperation and Development (OECD) and the United Nations have made the protection of privacy a major topic for study.

The British Columbia provincial government has enacted a right-of-privacy statute. A private-member's bill to circumscribe the activities of

"data banks" has been introduced in the Ontario legislature and an amendment to the Civil Code of Quebec has been proposed that would protect the privacy of an individual. A number of proposals were made by Professor Ed Ryan in his study Protection of Privacy in Ontario, undertaken on behalf of the Ontario Law Reform Commission.

In all this analysis and concern for the problem of privacy, one surprising fact emerges: privacy itself has never been objectively defined. It has been described many times, and everyone has a subjective version of what he considers his own privacy or personal property to be. One of the most succinct definitions, though not an all-encompassing one, was created by the 1964 Nordic Conference on the Right to Privacy: "The right to be let alone to live one's own life with the minimum degree of interference."

Professor Westin for example, considers privacy to be a basic human need related to the territorial imperative scientists have discovered in animals. In Privacy and Freedom, he writes: "What the animal studies demonstrate is that virtually all animals have need for the temporary individual seclusion or small-unit intimacy that constitute two of the core aspects of privacy." The extent to which privacy has been recognized and respected, however, has varied widely from one society to another. At one extreme, the Arabic language has no word for privacy; at the other appear to be Anglo-Saxon societies with their notion that a man's house is his castle.

Another train of thought, considering only Anglo-Saxon societies but in an historical perspective, leads to the unexpected conclusion that the average individual probably enjoys greater privacy today than ever before. Today most of us live alone or with only one or two other people,

in one or many huge, impersonal, urban complexes. Our grandparents mostly lived in small communities where anonymity and hence privacy were impossible; everyone knew all the sins of his neighbours.

Further, it must be pointed out that computers did not create the problem of privacy: Governments, commercial corporations, the police, maintained massive dossiers on individuals long before the digital computer arrived. What computers have done is to introduce several orders of magnitude of efficiency into the whole process of information gathering, manipulation and distribution.

As Communications Minister Eric Kierans put it in his keynote address to the Queen's conference:

> "This conference is a step, and no more than a step, in exploring the potential invasion and circumscription of privacy which may be brought about by the rapid development of computerized information systems and data banks. In this instance, there is a very clear potential social cost which must be matched against the quite obvious social and economic benefits of computerized data banks. It is precisely the kind of issue which we must explore and resolve if we are not to permit, without intending to or willing it, a wholesale technological pollution to match our industrial pollution - a technological pollution which could end up with us re-ordering our social behavior and priorities to suit the mechanical convenience of machines."

Taking part in the conference were some 150 businessmen, lawyers, computer scientists, economists, educators, sociologists and private citizens. Some participants apparently came convinced that there was no problem of computers and privacy at all and apparently hoped the conference would simply put the question to rest. A few suspected a plot - that the

conference was being held to justify the drafting of yet another batch of restrictive legislation that would put still more power in the hands of government officials. Still others appeared to be so eager to bring about sweeping, general legislation that they had not adequately considered damages that might result to the economic system and established institutions in the society.

This divergence of views suggests the conference planners had done their job well, that, as the conference Chairman put it: "The conference itself, to the extent that human frailty can do it, is representative of industry, of users, of interested individuals in the universities, in the legal profession and in government. It also, again within the limits of human frailty, is balanced between these different groups."(1)

Opening Thursday evening with a plenary panel session on "Privacy and Openness as Social and Legal Concepts" the conference proceeded through five more panel sessions interspersed with four meetings of workshop groups. The other panel topics were:

b) Data banks: existing technology and practice.

c) Data banks: direction of development resulting from needs and technology.

d) Objectives for securing privacy and freedom of information in data banks.

e) Legal and regulatory means of reaching objectives.

f) Professional and technical means of reaching objectives.

(1) For list of conference participants, see Appendix C. Some conference participants complained there were no representatives present from youth, from consumer groups or from the public at large.

For the workshop sessions, conference participants were divided into groups of 12 to 16 for a free discussion of issues raised during the panel sessions. Each workshop turned in a report of its views and recommendations on Saturday evening after the last workshop meeting. The conference secretariat then studied these reports and distilled from them a final summary report which was presented to the full conference in plenary session. Copies of the workshop reports were also then circulated among participants for verification. The approved text of the conference summary report is reproduced in Appendix A.

It was also explained at the plenary session that rather than produce a verbatim "Proceedings" of the conference, an edited summary report would be written and distributed to all participants. This report would attempt to capture all of the important, and much of the enjoyable, information and opinion that emerged in the position papers, the panel sessions, the question-and-answer periods that followed them and the workshop sessions.(1) And above all, it would attempt to put all this information into a coherent, readable form.

The following report is the result. Its format deviates somewhat from the chronological order of discussions at the conference, usually in order to bring together comments and discussion on what turned out to be recurring topics. In attempting to be comprehensive, the report may give the impression of wide disparities in the viewpoints of participants. Indeed, there were several major differences of opinion to be recorded. However, on most topics, a nascent consensus could be detected - either

(1) The list of position papers and background papers is contained in Appendix B. These documents are available, on request, from the Department of Communications.

through lack of argument or through an apparent synthesis arising from lengthy discussion. Most participants were truly astonished at the end of the conference to realize that such a wide area of consensus had been reached.

This report is divided into four chapters.

Chapter I deals with the problems of understanding privacy as a social and legal concept. Such an understanding is fundamental to any attempt to evaluate current practices that may invade privacy. It is even more important for those attempting to foresee future technological developments which may occasion even greater invasions of privacy. For example, it is well known that governments, school boards, doctors, police and several others carry out activities for various purposes and with various degrees of discretion which may result in invasions of individual privacy. But it is impossible to decide whether or not their practices are acceptable until a general notion of privacy is accepted. Furthermore, it is entirely possible that emerging technologies, when harnessed in the service of governments or doctors or others, may so change the nature of the activities of these groups as to make them become invasions of individual privacy. Again, a notion of privacy is a prerequisite to determining the rights and wrongs of this situation. The chapter concludes with a summary of the ways in which privacy has been acknowledged historically in the law.

Chapter II is about information. It brings together various notions about the power of information and the ways in which the development of "information systems" affects that power. For purposes of illustration, the operations of some information systems are described.

Some suggestions of ways in which information systems may be classified are also included in this chapter.

In Chapter III, the subject of the computer's impact on information systems is discussed in detail. Here are indications of the ways in which computers may alter information systems, for better and for worse, and also some discussion on the technical and economic feasibility of developing large-scale computer-based information systems.

Finally, in Chapter IV, the various proposals for action and the reasoning behind them are recorded.

CHAPTER I

PRIVACY: SOCIAL AND LEGAL CONCEPTS

"Privacy may be one of those things like beauty, truth and freedom - something that exists only in the eyes of the beholder." That remark, by Dr. Leon Katz, member of the Science Council of Canada and Professor of Physics at the University of Saskatchewan, seems to sum up the many frustrating attemps by conference delegates to come to terms with the notion of privacy. The subject of privacy as a social and legal concept was treated in depth by the conference's first panel but apparently not fully enough, for it surfaced again and again in workshop sessions and in post-panel question periods as delegates tried to come to terms with it. Many declared there was no point in talking about anything else until the issue was settled. The conference summary report does no more than list some of the major trends of thought:

> "Several workshops referred to the necessity of elucidating the notion of privacy as a legal concept or, indeed, to elaborate on a philosophy of privacy. Some doubted that this could be done except on an ad-hoc basis and others felt the concept varied with historical or social circumstances and should be left to the courts. Again, others reached the conclusion that the right to privacy should be expressed in the law and that it should be in accordance with the Universal Declaration of Human Rights."(1)

With the advantage of retrospect, one can detect from the many papers and discussions on this topic that attempting to define privacy may have been the wrong way to approach the problem. Rather, starting from the premise that privacy, whatever it may be and however it may be defined, is vital to and perhaps synonymous with an individual's sense of dignity, the problem is to find out exactly what actions offend an individual's or a

(1) See Appendix A for conference summary report.

group's or a country's dignity and then to do something about them. First, however, let us test the premise - that privacy is vital to an individual's sense of dignity.

1. Privacy and Dignity

> "We as an advanced society have always been invading privacy. We have always forced the poor, we've always forced the young, unwed mothers to bare their souls but it's only lately that the middle-class society has become concerned about privacy because it is their society that now stands a risk of being invaded."
>
> - Thomas L. McPhail, Loyola University.

One of the most striking examples of how the quality, indeed the nature. of a man's life can be altered by invasions of privacy, was given by Ontario M.P.P. Tim Reid, panellist and author of a private member's bill concerning data banks and privacy which he introduced into the Ontario Legislature in 1969. The example had to do with information collected and used, concerning high school students.

Reid pointed out that high school students, aware that comprehensive reports are prepared about them by teachers and school authorities, are under tremendous pressure to conform.(1) He described the case of a student leader to whom he sent a personal letter in care of the school principal's office. The student received the letter after it had been opened by school authorites. His dilemma: "If I make a fuss, someone will put on my record that I'm unreliable, a troublemaker." Reid then

(1) Prof. J. M. Carroll of the University of Western Ontario described the Ontario student record form. "It invades privacy to a greater extent", he said, "than do the records filled out by a convicted criminal being placed on probation, an individual taking a high security position with the Federal government or a recipient of welfare. It includes things like language spoken in the home, religion, occupation of parents, where the student does his work, how much homework he does, whether he has his own desk and numerous other items of personal information."

expanded this example to the larger society.

> "The student who knows information is being collected about him and who is concerned about having a good record so he can get into university and get a good job is just like the family man who finds out the kinds of information now being collected by investigative agencies. People are just beginning to understand how much is collected and they tend to react in one of two ways. They will fight if they can't be hurt. More often, they will say to themselves that it is better to wait for ten years until their children are grown up. (The period during which the family needs a good "credit-rating". In the meantime, they conform and opt-out of the fight to protect such pernicious invasions of their privacy.

Justice Minister John Turner, in answer to a question, distilled the essence of this point. "The right to dissent", he said "becomes a very difficult right to maintain if there aren't those areas in which one can discuss without the fear of being overheard. A democratic policy depends on a lot of confidential relationships, conversations, the ability to muster support in private, and so on."

Another example of how awareness of surveillance can affect an individual's behavior was given by Claude-Armand Sheppard, a Montreal lawyer and panellist at the 'Concept-of-Privacy' session. He described a hypothetical case of a married man who, unknown to his wife, frequents a bar popular among homosexuals. The man is, of course, aware that police often raid bars such as this one and that they probably note his presence there. If this man were charged with an offense totally unrelated to the fact that he sometimes went to that particular bar, asked Sheppard, would he not be reluctant to mount a strong defence for fear that the police might bring forward their knowledge of his activities in the bar and thus embarrass him

in front of his wife and family.

It was this kind of individual reaction to surveillance that A. E. Gotlieb, Deputy Minister of Communications, undoubtedly had in mind when he remarked:

> "The individual may come to feel to an ever-increasing extent that he is spied-on in an information-dominated society, and his behavior may be influenced to the point where he prefers to act in the same way as those around him and not set himself apart."

The result, according to Gotlieb, "would be an atrophied society whose members would show no initiative or willingness to innovate."

Surveillance, when it succeeds in recording information that an individual considers private, demeans that person's dignity. And the preservation of individual's sense of dignity, according to Justice Minister Turner, is of crucial importance to a democratic society:

> "The erosion of privacy is the beginning of the end of freedom. For privacy is the foundation of the principle of autonomy, at the core of human dignity. The right to privacy not only goes to the core of our being as individuals but also the core of our being as a society or state. A state that demeans its individuals demeans itself. A society that mocks the privacy of individuals mocks itself."

It is extremely difficult, however, to nail down just what people consider to be private and personal; to know which invasions will upset an individual's sense of dignity and which ones will pass unnoticed. An even when and if these unacceptable invasions can be discovered, there is the equally difficult legal problem of sanctioning their occurrence.

"Congestion is the only thing that will save privacy. Today, the most private place one can be is in his car in the midst of a traffic jam."

- Gordon Thompson, Bell Canada-Northern Electric Research Ltd.

2. Notions of Privacy

The simple act of asking what privacy means is a powerful indicator that a significant change in people's understanding of that notion has, and is probably still, taking place. In other words, people ask the question because they see around them evidence that activities they once considered private are, in fact, no longer private and/or things they once considered public have become private. Examples are easy to come by. One conference participant said that when he was young, his father wouldn't tell anyone how much money he earned. Now that information is public. On the other side, aspects of community living which were once shared among neighbours have now become private. How many people in high-rise apartment buildings have more than a passing acquaintance, if that, with their neighbours?

R. F. Linden, a computer specialist with the Federal Department of Industry, Trade and Commerce, claimed that the concept of privacy varies not only with time and between generations, but also between nations, between regions and between social groups. He said that in Germany, for example, people are appalled at the size and scope of North American credit information systems, considering that these wreak gross invasions of individual privacy. But they do not mind, as we probably would, reporting to the police each time they change residence. The Dutch, Linden continued, won't have social security numbers or their equivalent for at least three generations. The

reason: when Holland was occupied during the Second World War, the German Gestapo issued each citizen a number. And so, for the Dutch, social security numbers have come to be seen as a threat to the individual. The Danes accept that their government maintains a complete dossier on each citizen but they refuse to allow these dossiers to be computerized. Apparently, during the war, when the Danes wanted to hide someone, they could secure their efforts by stealing the individual's dossier. If the dossier were on a computer, that would be very difficult.

The common thread in each of these examples is the individual at a given moment of time confronted by a situation which may compromise his sense of dignity, indeed, his security through an intrusion into an area he considers to be private. The important point is that this evaluation takes place in the mind of the beholder. It is completely subjective. As the mind's sensitivities evolve under the influence of time, experience and culture, so the individual's evaluation of what is private and personal evolves. Privacy appears, above all, to be a dynamic concept, one that defies definition, except in terms which are also dynamic.

3. Measures of Privacy

If privacy is a dynamic concept, a major problem is to discover what it means to any given social group at any given time. For only when there is an awareness of consensus in a society about what is to be considered private can that society take legal action against those who infringe upon an individual's privacy. There emerged from the conference papers and discussions several suggestions of ways of measuring a group's beliefs about privacy. All appear to be based on a tension that exists in

each situation in which privacy is in play - a tension between those who would keep information private and those who would have it shared to a greater or lesser degree. Apparently, there is an immense variety of types of situations in which this battle between privacy and openness takes place, and undoubtedly several ways of categorizing these types.

The conference seemed to focus on two main groups:

a) those in which the individual wishes to keep certain personal information to himself while an outside agency, private or public, attempts to record it for any of various purposes.

b) Those in which the individual wishes to have access to information that governments or private information collection agencies would rather withhold.

In many situations, of course, both these struggles may occur at once. For example, a credit bureau may seek out and record information about a person that the person might not willingly have revealed. Then, the agency may well refuse to allow the individual to review the recorded information. And in almost all cases, it appears that the individual is pitted against large, powerful institutions within the society, such as government agencies, research establishments or corporations. And reconciling the rights and legitimate interests of the two sides is not an easy task.

Professor Thomas McPhail, a sociologist at Loyola University, Montreal, and a panellist at the session on securing privacy in data banks, posed the dilemma of the social scientists as a prime example:

> "Social scientists do definitely invade privacy. There is no doubt about it. All you have to do is refer to the classic Kinsey studies or the contemporary Johnson & Masters studies which are recorded in two books, Human Sexual Response and Sex Behavior in the Human Animal.

> As a social scientist, I am very much concerned with the definite need for Canadian legislation to protect individuals from the ruthless and undemocratic invasions of privacy by government, military or private and public agencies with little regard for human dignity or due process; but as a social scientist I am concerned also that in an overzealous attempt to protect everyone from everything that social science research may be brought to a standstill in many vital areas . . . The right to collect data, particularly in sensitive areas; for example, family, religion, income, illegitimacy, education, alcoholism, divorce, abortion, etc. is essential for some social science research."

Similar views were expressed by government planners, statisticians and businessmen involved in market research. Their argument is that they collect information only to detect social tendencies and trends and that they have no interest in relating particular information to identifiable persons. They promise not only to protect the individual's dignity but also to conduct research that will benefit the individual in one way or another.

While these arguments are impressive, they appear to have been advanced after the event. In other words, the planners, statisticians and others in this group appear not to have considered whether or not people like being the objects of research. Instead, having decided that their functions are important and legitimate, they have performed them without much thought given to the legitimacy of conflicting claims. As M.T.Pearson, general manager, Associated Credit Bureaus of Canada, said at one point, "No one ever asks the consumer what he thinks." For the purposes of measuring a social group's feelings about privacy in situations like these, it would appear essential to find out how far the individuals in that group are willing to allow various agencies to probe, even if anonymously and even if for the benefit of these individuals either singly or collectively. At what point, for example, do

these persons decide it is in their own good to keep information to themselves?

A. E. Gotlieb of the Department of Communications conceptualized the meaning of this decision by the individual as "the right to disconnect, or in other words, the right not to communicate." One of the fundamental principles of our society, he said:

> "is respect for freedom of the individual, a freedom that can express itself in a choice between communicating and not communicating. Every man should be free not to avail himself of information. But this is only one implication of the right not to communicate. It must also involve the right not to communicate involuntarily, that is, the right of the individual to restrict the use of information that has been gathered about him."

Another group of data collectors, led by credit and personnel agencies, only partially conceals the identity of the individual. But their justification is that their information systems are vital for the efficient operation of the economic system. Pearson claimed in his position paper that "Canadians enjoy a better standard of living than ever before because we are a credit-oriented society." And, he adds, "Without credit bureaus, it is reasonable to assume that individual business firms would be reluctant to grant credit without a long and costly search; many deserving persons, particularly average wage earners, would be refused credit because of insufficient data; and delays in obtaining credit would result in the loss of sales and decline of business volume." While this is undoubtedly correct, again it appears likely that individuals have not been asked their opinions. And the key question would be: At what point does a person feel the efficient operation of the economic system compromises his dignity? How much efficiency is he willing or even eager to

foresake in return for being probed less intensively?

Still other groups of data collectors, such as doctors, lawyers, police agencies, etc. each want personal data for different reasons and use it with varying degrees of discretion. In each case, the individual is presented with a challenge. Does he accept willingly that these agencies collect and use information about him or does he feel compromised by its disclosure in any way? Apparently, no one knows and no one has given much thought to the problem of finding out. But the answers are obviously vital for they become the measure of a person's expressed need for privacy to maintain his sense of dignity.

The other category of privacy-openness confrontations is manifested in situations in which the individual desires to have access to information that others would rather withhold. Again, A. E. Gotlieb, in his paper, conceptualized this desire as:

> "the right to communicate, or, in effect, the right to be connected. In a society dominated by information which is what we are moving towards, no individual should be required to remain apart from the automated flow of information. The disadvantages would be too great, and the gap created for the individual could become impossible for him to span by other means."

Today, this desire is most frequently articulated - and it was at the conference - as that of the individual to have access to information held by governments. Governments generally have a tendency to withhold information about their activities even when there is no reasonable justification for doing so. As Justice Minister John Turner, put it, "This is the tendency of governments to abuse citizen entitlements under the guise of privacy. In other words, government secrecy is sometimes legitimated as the need for a

government's right to privacy but which may well be a denial of the public right to know."(1)

The belief that there are abuses in this area was almost universal. Ten of the workshops agreed on the need for protection of freedom of access to information. And the conference summary report states: "this was regarded as being particularly important with respect to government information." Many conference participants believe this right of access to information should extend to other domains as well - notably to permit individuals to inspect credit and other personal information files and to obtain redress for inaccuracies. Others would go further, still others not as far. But there was general recognition of a danger that institutions can exploit privileged information to the detriment of individuals.

This danger develops from the concept of information as power, the idea that the exclusive possession of certain kinds of information confers upon the holder certain power. The overt use of compromising information about an individual to blackmail him is a simple example. Others, both more subtle and more frightening in their potential consequences, were cited at the beginning of this chapter. A related danger, to paraphrase Allan Gotlieb, is the widening gap between the few who collect and manipulate information and the many who are manipulated, particularly if they are aware they are or can be manipulated.(2) Enlarged, this gap could result in a paranoid, intellectually atrophied society. And, with the rise of sophisticated, electronic techniques for gathering, storing and securing information, the prospect of this

(1) "Paradoxically, an increase in government's privacy compromises individual privacy. Conversely, by stripping government and other institutions of their privacy, the individual's privacy zone grows."

- Hugh Lawford,
Queen's University

(2) See page 16.

gap widening appears to many to be a very real one. Hugh Lawford, professor of Law, Queen's University, described one of the many ways in which computers can widen the gap.

> Clearly, it is conceivable to create an information system under government control which permits only authorized officials to view only documents which they are authorized to see. Since the computer system can use transitory displays of information upon television screens in officials' offices, there need not be any unnecessary copies of documents. Since the system can record the name of every official who has viewed a document, responsibility for the unauthorized disclosure of government information can more readily be traced back to the particular official. A single system may serve a whole government department (and possibly even a whole government) through one centralized collection of machine-readable files. These central files do not require the intervention of a host of human file clerks, messengers, librarians and the like, and the internal government community responsible for custody of information can be shrunk to an extremely small group.

These two dangers - that institutions have sensitive personal information with which they can manipulate individuals and that this information may be concentrated in fewer and fewer hands - can be reduced in at least two ways. One is to force the would-be manipulators to make their information universally available, thereby stripping them of their potential power to blackmail or intimidate individuals. Another is to forbid the would-be manipulators from collecting information in the first place.

In some situations, of course, perhaps for reasons of national security, information must be gathered and must be withheld from the public. But Justice Minister Turner was the first to admit that these situations are few in number and widely accepted by the public. There may also be other

situations in which the public would prefer that information collections be kept secret; still others where the public wants the information kept confidential but claims a right to review its accuracy. In still other situations, perhaps the public doesn't care. But once again, no one seems to know what the public thinks or wants.

At this point, one is tempted to suggest that information collection agencies should stop whatever they are doing and run out and conduct a series of public opinion surveys. In so doing, they would find out how much information people will divulge and to what extent people want access to information held by others. Certainly, such a move would be a step in the right direction but it is fraught with dangers. One of the few initiatives in this direction was a research project undertaken by the Associated Credit Bureaus of Canada in 1968. One of the conclusions of this work, as reported by M. T. Pearson, general manager of the ACBA, was that "the public has a low level of awareness of the credit bureau function and an almost infinitesimal interest in the process of credit reporting."

Without wishing to impugn the efforts of the ACBA, this example points out a serious problem that will arise in any attempt to sound out public feelings on subjects such as this. In any such sounding, one could seek to discover what levels of privacy invasions and intimidation people will tolerate. And the many "horror stories" recited at the conference indicate clearly that many people have already quietly put up with a good deal of abasement through invasions of privacy. On the other hand, a far more difficult task would be to try and find out what limits on invasions of privacy individuals would consider adequate to maintain their sense of dignity. How, in short, do you provoke people to express accurately what

is needed to restore an element of their dignity that is being imperceptively whittled away?

A related problem is deciding what action should be taken even if accurate information can be acquired. One workshop at the conference came to the startling conclusion that the decision as to whether an individual should be allowed to keep information secret or be obliged to give it to responsible authorities should be based on "the greatest good for the greatest number" principle. This is startling because about a dozen people actually agreed that the principle of respect for minority rights, one which seems to be crucial in decisions affecting privacy and openness, should be ignored.

4. The Legal Status of Privacy and Freedom of Information

> There are laws that protect, and have protected for many years, some areas of an individual's private life. I am thinking of such things as the laws of property and trespass; laws that incorporate certain fundamental human rights; laws of libel and slander; laws that grant confidential status to information that passes between, say, a doctor and his patient; and laws respecting the monitoring of telephone conversations. In practice, however, these laws do not provide an adequate protection of privacy. In Canada, for example, the use of miniature radio transmitters and electronic eavesdropping devices is not regulated . . . The law is often blamed for being static and always behind technology. This criticism is probably justified. If it holds true for the future, the consequences may even be more serious than in the past.
>
> - A. E. Gotlieb,
> in a position paper

The laws cited above by Allan Gotlieb not only fail to provide "an adequate protection of privacy", as he puts it; in most cases they were not even intended to protect privacy. The law of libel, for example, is

intended only to protect an individual against unmerited defamation. It provides no protection against the exposure of sensitive information that is accurate! In Britain, the law forbidding wiretapping is not based on the individual's claim to privacy. Rather, wiretapping is prohibited because it is construed as theft of British Post Office electricity!

"The right of privacy is not one that has been given much recognition or protection in our law", Professor Douglas A. Schmeiser, of the University of Saskatchewan College of Law and chairman of a panel session on legal problems, argued. "It is not found in the Canadian Bill of Rights; it is not found in provincial bills of rights; it is expressly rejected in judicial proceedings, in most professional communications and in modern police practices." He was supported by Claude-Armand Sheppard, who declared simply, "The concept of privacy in law is relatively new. It is not unknown in Canadian law", he said, "but its recognition has generally been implicit rather than explicit. It has been dealt with in a piecemeal fashion and haphazardly."

Sheppard points to "token" acknowledgement of the principle the guarantee of mail secrecy in the Post Office Act, in various federal and provincial statutes prohibiting interference with telephones or wire-tapping; and in several provisions of the Criminal Code, such as those prohibiting the watching and besetting of individuals, dwelling houses or places of work and requiring a search warrant for an officer to penetrate into any private building. "In this connection, it should be recalled that a search warrant 'shall be executed by day, unless the justice, by the

warrant, authorizes the execution of it by night'".(1)

Sheppard also pointed out that Quebec law does not contain any specific provision dealing with privacy but that a proposed bill of rights contains a passage guaranteeing to every citizen a right to the protection of his dignity, his honour and his reputation as well as his right to privacy. Also, there is precedent, he pointed out, for using the general principles of civil responsibility in the Quebec Civil Code to prosecute invasions of privacy (see footnote below).

In summary, Sheppard and Schmeiser seem to agree with Professor Westin that privacy has been recognized in the past but the business of embedding measures in the law to adequately protect privacy has lagged behind technological developments.(2)

(1) Sheppard's remarks are buttressed by most Canadian writers on the subject. David Cornfield, writing in the University of Toronto, Faculty of Law Review, concludes that "although privacy receives some limited protection from the law of trespass, nuisance, negligence and copyright, no English court has ever given a remedy for invading the personal seclusion of an individual per se apart from his occupancy of land or his holding of some form of personal property." Another writer states "with some confidence that English Law does not recognize the right to be left alone. Personal privacy as such is not protected as a right, nor is there any correlative duty imposed on other persons to prevent them from infringing it."

One recent exception is found in the case of Robbins vs Canadian Broadcasting Corporation, where the CBC was found at fault for inviting viewers of a program to write or phone and "cheer up" a doctor who had written a letter to the CBC complaining about the program. Using section 1053 of the Civil Code, "Every person capable of discerning right from wrong is responsible for the damage caused by his fault to another, whether by positive act, impudence, neglect or want of skill", the Quebec Superior Court found that the CBC had committed a fault and was therefore responsible, but that there was "no need to attempt any precise definition of this fault".

(2) Westin, Privacy & Freedom, pp. 330-364.

Hugh Lawford, on the other hand, argued in his position paper at the conference that "The common law has been reluctant to recognize a right to privacy because such a right would endanger a more fundamental right of free speech. Such restrictions as the common law has placed upon the freedom to communicate information have been narrowly construed. For example, the legal remedies which the law gives for defamation of character are quite limited. Even if someone has spoken about me in terms which bring me under public hatred, ridicule or contempt, I cannot succeed in suing him if he can show that the words used were true." Lawford also pointed to the tendency of the courts to reject claims to shelter whole classes of information that could be used as evidence.

Whatever the historical perspective from which one views privacy as a legal concept, it is clear that the concept has, at present, little firm basis in Canadian law. Only British Columbia, among Canada's eleven major governments, has a specific privacy statute. Also, there is little existing legislation to limit the activities of agencies that might otherwise invade privacy. A significant step in that direction is, of course, Justice Minister Turner's wiretapping bill, introduced in the House of Commons in the fall of 1970. But on the whole, there has been little action to circumscribe the activities of information collectors and little thought given to the legal problems posed by the emergence of "personal information" as a commodity and a tool for privacy invasion.

Another related gap in Canada law is the absence of legislation providing for what Turner calls "a right to know". He explained:

> There is another side to the right of privacy which has not received the prominence it deserves but whose dimensions cannot be ignored. This is the tendency

> of governments to abuse citizen entitlements under the guise of privacy. In other words, government secrecy is sometimes legitimated as the need for government's right to privacy but which may well be a denial of the public right to know. If privacy is the foundation of democracy, the right to know is fundamental to any participation in democracy. The public cannot be expected to dialogue - still less decide - meaningfully if it is refused the very information which would make such a dialogue and decision-making possible.

Professor Hugh Lawford explained in detail what the absence of a right to information means to a citizen trying to deal with certain federal agencies. "Canada", he said, "has never enacted a clear law respecting clearance of documents and access to unpublished documents." This gap exists with respect to both archive collections and documents still in the possession of government departments, he claimed.

> "It is even difficult to discover who is responsible for granting permission to see government documents. Until fairly recently, a common assumption was that access to Canadian government papers was subject to a "50-year rule". That is, any document 50 or more years old was regarded as open to the public. Yet it is difficult to find any legal authority for the 50-year rule or for the shortening of the period to 35 years announced recently by the Prime Minister. Certainly there are files older than 50 years which the government refuses to make available to the public.
>
> A Canadian finds it impossible to know what law governs access to government files. He has no assurance that a department even has the personnel to undertake clearance of its files. Indeed, the procedure for declassification and release of government files (if there is one) has never been publicized."

While both Turner and Lawford concentrate on the idea that the absence of "a right to know", particularly with respect to government documents, is dangerous to the functioning of the democratic process, it

should not be forgotten that this omission also has the potential to create a threat to individual privacy. This is because government officials, in possession of information they refuse to divulge, may be in a position to manipulate individuals, groups or the whole society. As A. E. Ende of the U.S. Federal Communications Commission and a conference participant pointed out, "The real danger to the individual is from government activity in gathering information, maintaining files and using them. We can be affected by the opinion of powerful people with privileged information."

CHAPTER II

INFORMATION AND INFORMATION SYSTEMS

If nothing else, the preceding chapter should have suggested that "information" is the villain of the piece. Information is the "commodity" that an individual often wishes to keep to himself while others covet it. And information, in certain situations, is the tool of the manipulator or blackmailer. To extrapolate from Bacon - as everyone does who writes on this topic - information is power! To which should be added the all-purpose qualifier - "sometimes". Some information never has any power, some has power only for a short time, some has power only in certain circumstances. Thus, R. J. Bouwman, General Counsel and Secretary of British Columbia Telephone Co., could scoff at the alarmist posture adopted by many people on this topic.

> "I am a little worried about the fear that everyone here talks about, the fear of everyone knowing everything about you. I don't particularly care who knows about me, about my bank account or anything like that. And I just wondered if it is true that there is such a terrible fear or is this just something that we're building up in people?"

Those remarks serve as warning that the circumstances by which a certain piece of information assumes power (or loses it) vary considerably, even unpredictably. The power of a given fact may depend on that fact not being widely known, it may depend on the time that it is learned or on any or a combination of several other circumstances.

The relationship between information's power and its ability to help or hurt people also varies a great deal. Sometimes, information that

is helpful has power, sometimes is hasn't. Sometimes information with a potential for harming people has power, sometimes it hasn't. Sometimes, information has power regardless of whether or not it will hurt people.

Sometimes, information has power regardless of whether or not it is accurate. We know, for example, that personal information contained in school records or credit files has an enormous influence on our lives regardless of its accuracy. For one conference participant, the terrifying thing about some kinds of information is that people believe them. "We live in a pseudo-scientific age," he said, "and people tend to accord more value to so-called scientific data than they should." In fact, the strategic unimportance of accuracy in situations such as these seems to confer an extra power on already powerful information. This results, as Justice Minister Turner suggested, from the fear that develops in people - a fear born of "the awareness of the potential for the information not being accurate - the veracity of the information, the sources from which it may be derived, the biases from which it may be derived, the conversion of information corralled for one use and converted to another, the fact that there is no opportunity for rebuttal if that information is assembled without one's knowledge and thereby without one's consent."

On the other hand, people don't care about the veracity of what they apparently consider to be innocuous information. One conference participant reported the attempts of his company to verify the accuracy of information on its mailing list. He said that if the company pays return postage, 25% of those asked will reply to requests for verification of information. If the company doesn't offer to pay return postage, only 8% will respond. "75% just don't care anyway", he said.

In the midst of such disconcerting ambiguities surrounding information, at least one of its characteristics is fairly well understood. Fortunately, it happens to be the one with which the conference was most concerned. That is the tendency for information that already has some power to become more powerful as man's ability to store and manipulate it improves.

In other words, with each invention - hieroglyphics, the alphabet, paper, the printing press and so on - that has increased man's ability to store information, so the potential for an institution or an individual to accumulate information that can be used to advantage has grown. And more recently, with the development of mechanical, electro-mechanical and finally electronic devices for manipulating and analyzing information, this potential power has flowered even more rapidly, as is illustrated in a subsequent chapter.

Obviously, new methods and devices for storing and retrieving information were not developed in a vacuum. There were needs for them, needs expressed by people who explicitly or implicitly understood the value of collecting, storing and manipulating certain kinds of information. The result today is a proliferation of stores of information of all kinds held by all shapes and sizes of individuals and organizations. Some of these information stores, whether they are called filing systems, information systems or data banks, are kept on computers; some are kept in a man's head. Some, such as the telephone directory, have wide circulation; others, such as national defense systems, have extremely limited circulation.

The practices and problems of some of the information systems that

interested conference participants most are explored in this chapter. Also, ways in which information systems might be classified so as to separate the powerful from the innocuous are suggested. No attempt is made in this chapter to discriminate between manual information systems and computer-based systems. The problems considered here apply regardless of the storage and manipulation vehicle. The impact of the computer of information systems is the subject of a later chapter.

1. Some Information Systems: Existing Practices and Policy Problems

The conference was particularly interested in information systems containing information on people. Thus, discussion focussed on systems operated by credit and personnel agencies and by government and para-government agencies. The result was enlightening for, as Justice Minister Turner pointed out, we don't know much about them.

> The information systems dotting the national landscape in both the public and private sectors - and which are being increasingly integrated around computerized data banks - know a great deal about us but we know very little about them. What we need today is some hard data about the information systems and computerized data banks themselves, - i.e. - their number, type, nature, location and function; the ownership of these information technologies both in respect of nationality and public participation; what kinds of information are being collected, stored, retrieved, transmitted and disclosed; what measures, if any, have been already installed in these information systems to protect individual rights; how effective these measures are; and the operative trends in terms of information technologies and computer data banks in the Seventies.

Three panel speakers outlined the activities of credit bureaus, the Dominion Bureau of Statistics and school boards respectively. Open discussion elsewhere illuminated some of the practices of other data

collectors in our society.

M. T. Pearson, general manager of the 153-member Associated Credit Bureaus of Canada, spoke on the methods and policies of credit bureaus. He emphasized first the role of credit bureaus in society.

> "Outstanding consumer credit has multiplied five times since 1951 to an approximate total of $9,000 million today. ACB of C's 153 members provide more than five million factual and usually brief credit summaries a year, most of them by telephone, to more than 40,000 subscribers."

He claimed that member bureaus, however, do not grant or refuse credit, do not employ investigators who probe into an individual's background and habits, do not keep files secret from the individual concerned and do not provide credit reports to everyone who seeks them.

To protect the individual, ACBC policy requires service contracts between the bureau and subscribers certifying that "inquiries will be made only for the purposes of credit granting and other bona fide business transactions, such as evaluation of present and prospective credit risks. Service is discontinued to any subscriber who fails to honour these provisions. Subscribers pay an annual fee plus a charge for each credit report granted. To obtain information, a subscriber must identify himself by giving a special code number assigned on contract agreement.

"Furthermore, any consumer is able to find out what information is contained in his credit bureau file. He simply phones the bureau and makes an appointment. He is asked, on his arrival, to provide proper identification, then a member of the bureau's supervisory staff will go over the contents with him."

Pearson emphasized that files contain factual material only. He pointed out that credit bureaus have come to realize that a person's habits, political affiliations, etc. are not relevant. "The important thing is whether or not he pays his bills. Also, we won't store information we can't sell."

Thus, files contain a person's name, age, residence, previous residences, marital status, family, place of employment, previous places of employment, estimated income, paying habits and outstanding credit obligations.

"Bureaus may only record judgments and/or writs having to do with consumer debt; registered chattel mortgages, conditional sales contracts and convictions under provincial statutes and for criminal offences."

"Bureaus will report bankruptcies for 14 years, and collection accounts, judgments and court convictions for seven years."

Pearson also presented a table resulting from an ACBC research project in 1968 showing a low level of consumer complaints with the credit service (see Table I).

Finally, he noted that "no Canadian bureaus are currently computerized or have firm plans to do so". This despite the fact that ACBC's U.S. parent and other U.S. credit bureaus have put their files on computers.

"Several segments of the (Canadian) industry, in major market areas, have conducted studies but for volume or other reasons have not proceeded as of this date", he said.

TABLE I

Consumer Complaints Received and Interviews Completed

By Representative Sample of ACBC Members

1968

Region	Total # Of Reports 1968	Total # Of Complaints Received (Interviews Completed)		Total # Result Of Misunderstanding Of Business Function*		Total # Result Of Mistaken Identity		Total # Result Of Other Errors	
		#	%	#	%	#	%	#	%
Maritimes	317,717	887	0.28	423	0.13	89	0.03	90	0.03
Quebec	1,099,280	914	0.08	823	0.07	31	--	40	--
Ontario	1,662,587	3,114	0.19	2,015	0.12	47	--	69	--
Prairies	627,123	2,509	0.40	1,498	0.24	108	0.02	105	0.02
British Columbia	570,285	2,081	0.36	1,156	0.20	95	0.02	44	0.01
CANADA	4,276,992	9,505	0.22%	5,915	0.14%	370	0.01%	348	0.01%

* In nearly all cases, this was the belief that the bureau actually approved or disapproved granting of credit.

"Most members of the industry, however, recognize that computerization of some form, beginning in major markets, is inevitable, and largely a matter of volume, equipment economics and investment payout. On this basis, it is reasonable to assume that a significant proportion of the Canadian industry will be computerized in 5-10 years, and some major markets sooner than that."

Pearson's remarks pertain mainly to the Associated Credit Bureaus of Canada, a group of "in-file" reporting agencies. Subsequent discussion illuminated the activities of other participants in the personal information collecting industry. Professor J. M. Carroll of the University of Western Ontario, pointed out that, "for all practical purposes", there are three such organizations in Canada, the others being Dunn & Bradstreet, concerned primarily with businesses and large investors, and The Retail Credit Co. of Canada. Carroll emphasized that it is mainly The Retail Co., that carries out investigative work on individuals for the use of insurance companies and the like. He called this kind of activity "bedroom or bistro spying." All of the agencies, he added, are headquartered in the United States.

Carroll also disputed Pearson's claim that an individual can review his file.

"He has said that a subject has the right to review his file but it would be misleading if one would think that you can walk to a credit bureau, get the document, which they call the docket, and hold it in your hot little hands and examine every statement made about you. This is just not done."

"You make an appointment", Carroll continued, "to review a file at the credit bureau - this is Mr. Pearson's organization. I do not know if the

other organizations have even gone this far. Now, the manager of the credit bureau holds your file and he says, 'Mr. Jones, now just what was there about your credit status that is troubling you?' In other words, he's playing 'twenty questions' with your file and he is putting you in a position where you have to volunteer information, perhaps derogatory information, that might not be in the file in the first place. I say that this right to review a file is not that; it is only the right to subject yourself to a personal interrogation."

To which Pearson replied: "The file is in code for confidential purposes. He wouldn't understand the file anyway so we have to interpret it. It would go like this. It might say, 'F - 100 - 1 - 69 - 1,000 - $60 - 800 - 01'. The main point here is that on the docket are confidential codes that the member uses to phone in. Now, if we hand somebody the docket and he picks up the code, he can go out and give the code to some of his friends and he in turn can phone into the bureau."(1)

Some of the personal information handling activities of the Federal government were outlined by T. J. VanderNoot of the Dominion Bureau of Statistics.

He pointed out that the Canadian Statistics Act guarantees to the individual that no harm will come to him as a result of his compliance with the Act in providing information to DBS.

(1) For further information on the personal information-gathering industry in Canada, see Gibson, R.D. and J.M. Sharp, Privacy and Commercial Reporting Agencies, Legal Research Institute, University of Manitoba, Winnipeg, 1968.

> The protection of individual returns covered by the Statistics Act includes the following three major provisions: (1) the individual returns furnished by persons, businesses, etc. will be used only for statistical purposes and not made available for taxation, regulation or other administrative action; (2) the returns will be handled only by sworn staff to DBS; and (3) the data will be published only in a form which will not permit, without authorization, the identification of data relating to any individual form or other respondent.

Despite precautionary measures taken to ensure that these protections are respected, VanderNoot noted there are difficulties, particularly in the area of residual disclosure.

> This occurs when two or more sets of data taken <u>together</u> could allow the identification pertaining to an individual respondent even though there is no direct or intentional disclosure. The trivial example occurs when an entry in a table is blanked out but which can be deduced from the marginal totals and the other entries in the table. A less trivial example is the publication of certain industry totals by province when one cell is dominated by a single respondent.

The "residual disclosure" problem illustrates a point made during a workshop session. Information contained in a data bank on an individual need not include the individual's name in order to be identifiable.

Another danger is implicit in DBS using information collected by other government agencies and departments of administrative purposes.

> This is an increasingly rich source of statistical information since the administrative activities of modern governments encompass ever wider spheres. Yet the public is concerned that the accumulation of information about individuals within one agency will allow the linkage of information from various sources and thus create the feared 1984-type dossier.(1)

(1) For further discussion of the "linkage" problem and an example of it in action, see R. H. Donnelly case, Chapter III.

A para-government data collection agency that received some attention was the school system. Ontario M.P.P. Tim Reid, explaining in a panel session the reason why he introduced a private member's bill on data banks, recalled that:

> "I was becoming increasingly alarmed at what was taking place with regard to elementary and secondary school student records, particularly with the advent of report cards during the 1960's on which the teacher was encouraged to express very subjective comments on the pupil's social behavior in and out of class, his relations and bad and good habits and so on. In other words, I was alarmed that very subjective comments of a psychological nature were being made by amateurs with no training."

Reid was concerned not only with this activity but with the fact that these observations are recorded on student record forms that follow the student throughout his academic career. Furthermore, he argued, supported by Professor John Carroll of the University of Western Ontario, that the distribution of these students record forms is often not adequately restricted.

As Carroll put it: "It's not unheard of for the principal of a school, in answer to a request for information on a student, to xerox a copy of the student record form and send it out to the individual making the inquiry". But he also pointed out that, "there are already laws regarding the confidentiality of this document. I believe it is under the Secondary Schools Act. So, you see, we are talking about more legislation but we don't even have the mechanisms to enforce the protections we already have written into legislation."

Reid also cited the instance in Toronto in June, 1968 when police asked for and received the student record form on a 17-year old former high school student who was to be a Crown witness in a court case.

Valuable insight into the activities of yet another group of data collectors - social scientists - was provided by Thomas McPhail of Loyola University. With one example from his own experience, he pointed out both the value of social science research and some of the latent dangers to both individuals and the scientists involved in it. The example deals with marijuana research.

> I designed a questionnaire along with a couple of colleagues and at question eight, it says, "Have you ever smoked marijuana?" Then, further questions are, 'how many times?' and 'how many times have your friends smoked it?' Now, on the top of that questionnaire, it says 'this questionnaire is both anonymous and the data will only be reported in agregates.' This is very sensitive research but the findings, I think, provide us with insights about human behavior that are very vital in terms of decision-making. For example, we have found that among freshmen, 12% have smoked marijuana. By the time you go through first, second, third and fourth year undergraduate, two-year masters program and a three-year PhD program, it goes up as high as 80%. In other words, the Federal legislation as it is designed today, if it were enforced, would put most of the intelligent young leaders of tomorrow in jail. I think it's this type of research that we need and it's this kind of research I'm afraid may be closed off.

Asked if the police authorities could lay any claim on his data in this research project, McPhail answered, "they probably could force me in some legal way but if I became aware of this I'd destroy the data first."

2. Classifying Information Systems

The purpose of the conference, of course, was not to itemize the information systems operating in Canada today. The focus on some specific information systems above, however, helps to indicate some of the problems that arise in dealing with them, even if and when they are itemized. One

point that should be clear, for example, is that the term 'information system' can cover everything from the telephone book to the RCMP's criminal files, from Eaton's catalogue to a company's confidential customer list or a school board's file of student histories. And any attempt to deal with them all collectively will almost certainly lead to some bizarre traps. As an example of what can happen, Hugh Lawford showed that the strict wording of Tim Reid's private member's bill on data banks would render illegal the publication of telephone books![1]

"If you look at the bill", Lawford said, "I suppose that when you compile a phone book, you are keeping 'a filing system that records and stores information'". He then showed the phone book would qualify under section 3E of the Ontario M.P.P.'s bill because it is sold, and under section 4 because it is 'a data bank that contains personal information about identifiable persons'. Lawford concluded triumphantly with the thought that if someone discovers any incorrect or out-of-date data in the phone book, he can order the phone company to expunge it or correct it immediately or face a $10,000 fine.

Another example of how legislation, if drafted too widely,could do more harm than good, is the possibility, raised by some conference participants, that an individual's personal files could become subject to regulation - including scrutiny by those about whom the information is stored - on the grounds that 'personal files' constitute a data bank.

Examples such as these indicate that a way must be found to classify information systems and to assign names to the different classifications. Somehow, the sensitive must be separated from the innocuous, the information

(1) See Appendix IV for the text of Reid's bill.

systems with restricted distribution must be separated from those that are open, and so on.

In a position paper on the classification problem, Professor C. C. Gotlieb of the University of Toronto and Program Chairman of the conference proposed to classify information systems according to three characteristics: the source of the information, the extent of distribution of the information and the method by which an individual can (if he can) inspect the information about him that is stored.

For data sources, he noted that information can be supplied either by the individual or from public record or from other sources, "other" being defined by exclusion. The only problem area here, he noted, is clarifying what is meant by 'public record'. For example, do vehicle registrations, records of criminal convictions, voters' lists and so on all belong on the public record? Gotlieb cautioned: "Careful thoughtwould be needed to choose the list and it would have to be reviewed in the light of experience."

Under the 'inspection' classification, he suggested that, depending on the system, the individual either has an automatic right to inspection, in which case a copy of information held on him is sent to him automatically periodically or he has a right to request to inspect the information or he is forbidden to see his file altogether.

As for extent of distribution of the information, Professor Gotlieb put forth two categories, internal and external, but readily admits these are "the most difficult to define".

> Generally, internal is intended to mean that distribution of information is restricted to the company or institution which maintains the information system unless there

> is explicit permission of the individual about whom the data pertains, in every individual case, to transmit it elsewhere. However, in the case of government, federal or provincial, the organization is so large that it would be necessary to be much more precise than this, if the term 'internal' were to have any validity. If it turned out that it were not possible to define internal distribution with enough precision, it might be necessary to consider distribution for specific items of information rather than for the whole contents of the systems.

Professor Gotlieb then gave some examples of classification that would be assigned to familiar information systems. A payroll file is composed of data collected from 'other' sources (i.e. not the individual and not public record); it has only internal distribution; and the individual can, presumably, inspect it on request.

A police file is also made up from "other" sources, but it has external distribution and is not open for inspection by the individual. Who's Who is compiled from data supplied by the individual, it has external distribution and the individual has an automatic right to review his file.

> "Most of these information systems have a long history of use. Regulation of information systems could proceed first by identifying those of the type for which the individual has no right to scrutiny but which have external distribution. For all others, no regulations would apply. This would in itself encourage those operating systems to make their data open for inspection to the individual concerned, and to restrict general disclosure if possible, so that regulations would not apply."

In his remarks at the conference, Gotlieb added: "The whole purpose of the mechanism would be to indicate a very wide set of classes of systems on which generally no regulation or licensing would be needed. The whole point of the classification systems is to remove from any licensing need practically all the information systems that are operated, even about people."

The idea of classifying information systems was a popular one at the conference, although it emerged more in an awareness of differences between various types of information than in an understanding of what can be done about these differences. For example, one workshop suggested there is a vital distinction to be made between subjective and qualitative information on the one hand and objective, quantitative information on the other. It also noted a distinction between information that is collected for research purposes in which individuals are not identified and stored personal information that can be traced back to the individual. Another workshop, although in favor of complete disclosure of government and corporate information, recorded the following stumbling blocks:

> "Information relating to the future operations of companies, such as project capital expenditures, competitive information within the industry, etc. cannot be disclosed without jeopardizing the company. Other information, such as proposed location of highways or that affecting the stock market must be withheld."

It is likely that most, if not all, of these differences could be accommodated if the principles of Gotlieb's classification system were applied. Gotlieb himself emphasized that he was attached only "generally" to the classifications he set up, not to the specific classification suggested. One general area of disagreement, however, might be over the use to which information is put. Gotlieb, for one, was not interested in how information is used. "Let me point out", he said, "that I do not try and classify according to how information is used. I think that one of the aspects of information systems is that they have all kinds of uses that you didn't think of. And to try and expect that you can predict all the ways in which you can use it is probably not too productive."

If the workshop reports are a fair indication, his view is not widely shared. Three workshops noted that the uses to which information is put are of great concern to people, although none offered any reasons for this. Examples given included the use of personal credit data for employment purposes and the fear that confidential communications to doctors, priests and lawyers might be used for other purposes. Another workshop complained about the sale of magazine mailing lists. One workshop, however, came to the conclusion that people, in giving out certain types of personal information, waive the right to restrict its use. No examples were given. Dr. Willis Ware of The Rand Corporation argued in one workshop that the apprehension of use of information by third parties may arise simply because "we are afraid of the future. This is the emotional failing in all of us", he said. "We are worried about the gathering of medical information, for example, even though we're better off as a result of it. Why not reveal the identity of the individual?" But Ware also suggested data bank operators should be forced to declare the uses to which they put their information

Chapter III

COMPUTERS AND INFORMATION SYSTEMS

"I'd be very sympathetic to recognizing a right of privacy for computers too."

- A.E. Gotlieb

"A computerized system can administer injustice far more efficiently and far more quickly than any manual system."

- from a workshop report

"Computers are big, expensive, fast, dumb adding-machine-typewriters", according to Robert Townsend, author of Up the Organization. Perhaps. But this definition conspicuously omits the two other characteristics of the computer that cause it to affect traditional approaches to information systems. These are the computer's abilities to store vast quantities of data and to retrieve, sort and analyse that data under programmed control at lightning speed. John J. Deutsch, principal, Queen's University and chairman of the panel session on legal and social concepts of privacy, explains:

"in the past, we've had a protection from the limitations of the written word. While a lot of information could be collected, it was cumbersome, it was difficult to find, certainly difficult to find quickly, and this has given the individual a good deal of protection as far as privacy is concerned. It was like looking for a needle in a hay-stack. Well, what's happened now is that we can indeed find the needle."

Perhaps the best illustrations of the computer's ability to find needles in haystacks was that described to the conference by T.J. Vander Noot of the Dominion Bureau of Statistics. He said that a U.S. marketing

firm, R.H. Donnelly, Inc., brought together available public information on individuals living in a certain district. The information sources used were the enumeration area statistics from the census bureau, the telephone book and the auto registration list sold to them by the state. All this information was fed into the computer and correlated. And, from the results, "they were able to infer a great deal about the families living in the area they were interested in", Vander Noot said.

"I would point out", Vander Noot continued, "that the invasion of privacy is not just a question of dossiers or the illegal collection of information. But as social science itself becomes more sophisticated, perfectly legal means can be used to build up files of information about a person which is an invasion of privacy. And I would defer to the lawyers the question of how a series of perfectly legal actions can result in an invasion of privacy."

As luck would have it, a lawyer, Allan Gotlieb, took up the challenge, answered the question and showed that there is even a legal principle to support the suggestion that computers can bring about a qualitative change in information systems through a quantitative increase in capacity and manipulative power.

> "I can remember the story a law professor once gave as explanation of the relationship between what is legal and what may become illegal. A farmer keeps one pig and this is perfectly permissible; he keeps two pigs and it's permissible; three pigs and it's permissible, but at a certain point he may keep sufficient number of pigs that the pigs become a nuisance in relationship to his neighbor. So that at some times, information or actions which in themselves in isolation may be perfectly permissible can by society be regarded as changing in quality and their character in a certain combination. I

> think for example, that it is quite possible that under the laws of a given jurisdiction, the legislators may say that there shall be no bank of information formed on people by public or private (agencies) of a certain character or of a certain type even though the information may be public or, in large part, publicly available. I'm not advocating such an approach but I think it is certainly likely to happen in relation to the formation of general data banks on people by governments."

1. How Computers may Become a Nuisance

The conference summary report records "the predominant opinion" that the computer can indeed alter the "quality" of the invasion-of-privacy problem through its impact on information systems. The R.H. Donnelly case cited above by Vander Noot presents one way in which this can happen; that is, through the use of a computer to sort, compare and integrate various data files so thoroughly as to create a qualitative change in the data itself. But there are several other ways in which the computer can affect information systems and, in the process, either directly or indirectly, affect individual privacy too.

Consider, for example, the following prediction by Douglas F. Parkhill of the Department of Communications:

> "The technical advances that had made possible the information utility[1] have dangerously magnified the power of both governments and private organizations to keep all of us under close surveillance. Together, the various data files of the different (systems)--medical, educational, financial, legal, law enforcement, etc. could make available in a conveniently accessible form a complete record from birth until death of even the most private affairs of everyone. In the absence of adequate controls, this could create a dangerous menace to the right of privacy, and, if carried far enough, to a society in which conformity would become the price of survival."

---

(1) A term used by Parkhill to describe the massive computer-communications systems he predicts will be prominent in the near future. See below, page 55.

While the computer in this instance is doing much the same things as it does in the Donnelly example, a completely different legal problem is involved. What Parkhill alludes to is the possibility that governments or private organizations will integrate already confidential data files containing personal information, perhaps in the name of efficiency or money-saving, but nevertheless resulting, willy nilly, in a bank of personal dossiers that individuals, had they been asked, might never have agreed to establish.

A third way in which computers may impact information systems is implicit in Principal Deutsch's reference to being able to find the needle in the haystack. Simply because of the computer's immense memory and its manipulative powers, information systems can be built and used today that could not have been contemplated in the past. And many existing information systems, if placed on a computer, would become instantly, for these reasons, more powerful tools.

As A.E. Gotlieb noted, "Before the advent of the computer, files on the various activities of an individual were incomplete and separated from each other because too large a mass of information simply could not be manipulated economically. The computer, however, makes it possible and economic to store, combine and transfer masses of data."

A fourth way in which computers may affect information systems and, obliquely, privacy, is through their tendency, cited emphatically by Hugh Lawford, to turn previously 'free' information into a commercial commodity. "Because computer-based information systems are expensive and

can be controlled in a way that the flow of private paper cannot", Lawford argued, "Ithink that there is a tremendous pressure towards having information become an economic commodity.[1] So that it is possible to say that every time someone looks up a law on a computer data bank he should be charged a fee." Lawford also commented that in seeking legal documents from governments for use on his data bank, he noticed that they have begun to ask for some "economic benefit" for providing this information in a way they wouldn't have done in the past.

The implication is that this cost element, if it becomes generally accepted, could become another factor in expanding the gap between those with the power (and the money) to manipulate information and those who are manipulated.

Finally, Claude-Armand Sheppard, in his position paper and in direct remarks at the conference cites a fifth way in which computers alter information systems and, in the process, upset people.

> "To put it crudely, it is the fear of being ruled by computers. You and I know that this is a great over-simplification. We know that computers are really most suited for repetitive tasks. In fact, it has been said that computers don't think, don't make decisions, don't set policy. Don't they really? Most decisions which any administration has to make really consist in the application of relatively plain rules to facts which are equally simple. But to the individual concerned these simple, almost mechanical, decisions may be of the utmost importance, for they determine his rights, his security, and vital aspects of his life. Yet these are the decisions which are most likely to be entrusted to computers.

---

(1) Even more so when there is a telecommunications link between the "customer" and the computer system.

> Up to now, the citizen's main contact with his government has been in areas such as taxation, social aid and so on. Yet these are the areas that are being taken over by computers. Don't underestimate the anguish this will create in people."

It must be emphasized - indeed, it was emphasized several times at the conference - that these are, for the most part, ways in which the computer, when and if applied to information systems, has the potential to bring about invasions of privacy where none existed before or to exacerbate existing privacy invasions. Today, as M.T. Pearson pointed out, no credit bureau in Canada uses computers to store its information. Only governments have significant personal data files on computers but even there one finds curious gaps. The R.C.M.P., for example, still does not have an on-line criminal data file[1]. In short, the state of the operational art is, as usual, somewhat behind the technical state of the art. Nevertheless, there was considerable debate at the conference both on the technical and economic feasibility of harnessing computers to most information systems.

2. Financial and Technical Feasibility of Computerized Information Systems

Three conference panel speakers, B.B. Goodfellow of IBM Canada Ltd., D.F. Parkhill, Assistant Deputy-Minister, Planning, Department of Communications and John M. Russell, Vice-President, Systems Dimensions Ltd., Ottawa, spoke on technical and financial aspects of computerized information systems. In addition, there was limited discussion in workshops, but no major points are raised that are not covered in the three speakers' papers.

---

(1) One is, however, now under development. The RCMP announced in September 1970, its intention to develop an on-time data bank containing information on stolen vehicles and on criminals. The system will connect to the U.S. Federal Bureau of Investigation's National Crime Information Centre (NCIC) in Washington, D.C.

In general, Parkhill claimed that computerization of information systems is not only technically and economically feasible, it is already happening "at a phenomenal pace". Russell and Goodfellow, for their part, concentrated on pointing out technical and economic obstacles to the rapid emergence of computerized information systems.

"For the rest of the decade at least", Parkhill argued, "the most significant developments in information systems will arise from the merging together of the previously disparate disciplines of computers and communications to create those new forms of social endeavour that we call information utilities."

And he described several technical advances that have made this possible.

1. It is now technically feasible to bring the full power of a large-scale computer complex to anyone in the world who is served by suitable telecommunications facilities.

2. The interaction between the central computers and the remote user is essentially instantaneous so that the user receives service that is indistinguishable from that which he could receive if he were physically present in the same room as the computers.

3. The cost to each user is but a small fraction of what it would be if the same services were provided by individually owned computers.

4. Each subscriber can be provided with expandable, rapidly accessible private files that are reasonably well protected against unauthorized access.

5. The intellectual achievements and data collections of many individuals and groups can be pooled in large public files so that their contents become simultaneously available on demand to all customers of the system.

6. The technique of time-sharing has made direct dialogue between man and computer economically practical.

Parkhill then described some information systems that will be computerized in the future, and suggested some of the effects this computerizing process will have on these systems. He cautioned that "any complete list of possible applications would resemble the index to the Encyclopedia Britannica", but offered a preliminary list of some of the potentially important ones (see Appendix 5).

Perhaps the most important of the future computer-based information systems described by Parkhill are those intended for pedagogical purposes.

> "In the long run, nowhere will the impact of the computer utility be felt more strongly than in the area of education. Both the form of the school and the role of human teacher will undergo drastic changes as "fireside computer consoles", universal electronic encyclopedias, teaching utilities and academic administrative utilities come into widespread use. For one thing, the concepts of grades and of classes based on calendar age may have to be abandoned. In their place will be a system of independent tracks for each student, according to his individual performance. In fact, with the advent of domestic computer utility service, there is no reason why much of a student's instruction and study could not take place at home. The time at school could then be devoted to laboratory work, group discussions and seminars and individual consultations with the human teachers."

John Russell, Vice-President, Research & Development, Systems Dimensions Ltd., Ottawa, in a panel presentation, presented some of the technical and economic difficulties and limitations in creating large on-line, computerized information systems. Russell claimed that, "using currently available technology, no significant storage capacity limitations present themselves to the designer of an on-line information service".

> "Direct access mass storage devices presently offered for sale can make available to today's computers upwards of one trillion characters of information at a capital cost of approximately $10 million. Such a capacity would provide for approximately 10,000 words pertaining to every person in Canada at a capital cost of approximately 50¢ per person".

These data files could be stored far more cheaply, Russell noted, if they were put on off-line tapes rather than direct-access devices. "The above hypothetical files, for example, would be contained in approximately 25,000 reels of conventional computer tapes at a capital cost of less than 5¢ a person."

One of the major areas of technical difficulty in on-line systems, he claimed, is in the speed of access to information in the files.

> "Although the access times and data transfer rates may be quite high, when the designer takes into account auxiliary operations such as access request queuing, location directory searching, field password verification, privacy transformations, record rewriting and directory updating, he would consider himself cavalier to predict much more than about one thousand accesses per hour. This means that just one of the possible data bank access applications alone, motor vehicle registration for example, could tie up the system completely (three million vehicle registrations spread over 300 days = 10,000 registrations per day or 1,000 registrations per hour).

Russell added that the access-time problem is more acute in data banks used for 'specific' purposes than in those used for statistical purposes. In other words, when data files are accessed for purposes of statistical analysis, they can be drawn one after another in their natural physical sequence from the storage device. However, in cases where specific data is required, an individual (time-consuming) search is required for each item.

Russell also focused on some start-up problems that any would-be data bank operator would incur. For example, "the building process will generally require a manual conversion involving the transcription of the records to machine readable form. Perhaps the first and most immediate danger to the individual lies in the difficulty of ensuring adequate quality

control during large-scale conversion programs. And because transcribed records of an individual may not come in to actual use of months or years after the transcriptions, errors introduced at that time will tend to be difficult to right." He also claimed that this transcription process is "extremely expensive" and "in many cases, this cost alone could prohibit the transcription."

A design problem, which Russell discussed briefly, is whether to have one centralized data bank or a network of smaller, distributed data banks. Against the distributed option, Russell pointed out the high cost of transmitting data from one centre to another for - say - analytical purposes. And he cited the following hypothetical example:

> "An authorized researcher working out of one of the regional centres such as Quebec City wishes to study current health patterns of families in Ontario and Quebec. Having in hand a tape file derived just last week from the Quebec City data bank, he asks for the corresponding file from Toronto. Stressing the urgent nature of his research (e.g. mercury pollution), he asks for and receives permission to have the Toronto file forwarded by leased common-carrier communications facilities.
>
> "Now, the Ontario health records file may happen to contain six million records of 200 words each (roughly 50,000,000,000 bits). Since, in the current state-of-the-art, data transmits at a maximum of about 50,000 bits per second, our researcher in Quebec City will wait some two weeks for his data!
>
> "Although perhaps the transmission cost was not important in this instance, it is interesting to note that under current tariffs, the common-carrier tolls would have exceeded $7,000. Ordinary air express services could have been used to ship the tapes in less than one-tenth of the time at less than one-tenth the cost!"

To Russell's remarks must be added those of B.B. Goodfellow of IBM Canada Ltd. Goodfellow spoke mainly on the anticipated technical

developments in computer design in the near future that will impact the technical and economical viability of computerizing data banks.

"Today", he said, "we can visualize the technologies that will take us to absolute limits in central processor performance. By the mid-1970's it is reasonable to project 1- to 2-nanosecond systems and by the early 1980's, we should attain an order of-magnitude improvement with circuits in the 100-picosecond range. This achievement would appear to represent a limit for practical systems for some time beyond that period for the linear machine."

Goodfellow warned, however, that "based on the very limited experience with the design of current information systems, it is projected that search times (CPU to core) will have to increase between a thousand and five thousand times to make even relatively simple information systems practical." And, he said, "the projections of circuit improvement do not support such increases."

Also, in the organization of computer processors, Goodfellow claimed: "The current indication would be the development of multiple processor systems operating under the control of a master operating systems. A number of breakthroughs will have to occur in this area before system performance will satisfy the implied requirements of many of these proposed data banks."

Again in the area of bulk storage media, he noted that while there is no limit to the amount of information that can be stored, "It is an unfortunate fact that increasing storage generally increases access time." He foresees improvements in storage media over the next decade, to the

point where "very large systems (i.e. with on-line storage in the range of a billion characters or more) will be practical for the expansion of many applications in operation today, but they will have unacceptable access times to operate in realtime mode. Some of the new technologies may overcome the basic limitations encountered today but these systems appear to be beyond a ten-year forecast."

3. Security of Computerized Information Systems

Just by being themselves, computers can bring significant changes to information systems that may affect personal privacy. But computers and computer men aren't always themselves, don't always do what they are supposed to do. They make mistakes, they may not have adequately considered a problem and, in the case of computer men, they may become sloppy, negligent or simply dishonest. As a result of any of these eventualities, sensitive personal information stored on a computer may be distributed to someone who shouldn't have it or may be corrupted. In either case, personal privacy could be unjustly compromised. Steps taken to avoid such eventualities fall under the general rubric of security in the computer environment - a topic of considerable concern to many conference participants and, one suspects, to the public at large.

As a list of security requirements provided by Dr. Willis Ware indicates, the steps to be taken are considerably different from those in a non-computer environment. He cites five requirements.

1. Physical protection of the computing central and demountable storage media.

2. Communications should be protected by some form of encryption or physical protection of circuits.

3. A multi-user system must have hardware safeguards to prevent a user from upsetting the monitor program or software safeguards.

4. Software safeguards are needed to control user access to files and make audit trails, alert staff to unusual situations, etc.

5. Administrative and management security controls must be adequate.(1)

Given that these various approaches to security in a computer environment are followed up, the question remains as to whether computer-based information systems are or will be more secure than manual systems. The question is, of course, largely academic because there is as yet little experience in the field. Here, however, is a sampling of opinion and evidence from various conference participants.

B.B. Goodfellow of IBM Canada Ltd. argued that, "while technological developments may represent a potential threat to privacy, this same technology may be even more important to use in the protection of privacy. Whether we like it or not, our lives are not very private today and I am convinced that computers and automated data banks offer the potential for greater protection of our privacy than the threat they present to its invasion."

Concrete evidence for this idea appears in M.T. Pearson's paper on the operations of credit bureaus. "It is our contention", he said, "that computerization will in fact promote greater accuracy and confidential treatment of file information."

Pearson went on to suggest what some of the specific effects of computerization of credit bureaus would be:

---

(1) Legislation or regulation draftsmen may, or may not want to consider the irony of a computer system operator invading the privacy of his employees in order to protect the privacy of his customers.

"Computers are vehicles by which many credit bureaus' files can be consolidated into one metropolitan trading area. To the credit grantor, it means he can call one location to get information on potential customers in the total trade area which he services. To the consumer, this means a much quicker opening of a new account since the credit bureau would no longer have to mail a request for information to another city in those cases where the consumer has recently moved.

"Computers can control against errors more efficiently than is possible with manual systems. For example, more checks for reasonableness of data input are contained in the computer systems than are possible on a manual basis. Computers permit an automatic interface between the automatic billing systems of credit grantors and the credit bureau's files. Computers for credit reporting are all on-line systems. Correction of errors can be entered in these systems as quickly as they could be entered in any manual system. With computers, there is a new ability to go through files quickly and delete older information that should no longer have a bearing on the person's ability to pay.

"Computers permit bureaus to have greater checks to guard against misuse of their files than is possible on the manual basis. In the U.S. Associated Credit Bureaus computer package, Credipak, a complete audit trail is maintained on every access and change to the file, including an operator's identification. No terminal can access the files until such terminal is activated by a supervisor and the assigned operator has identified herself on that terminal. Any terminals placed in credit grantors' offices for direct access to the bureau's files are not permitted by the computer software to make changes to files other than to indicate that an access has been made. The system also produces lists of all significant changes made to files which require some supervisory review."

Pearson's contentions were further supported by David Booth of I.P. Sharp Associates Ltd., Toronto. Booth described in detail the secutiry system incorporated into the company's computer time-sharing system in Toronto. Like the Credipak system, the I.P. Sharp system aims at providing a high degree of file integrity and security.

The system provides each user with a 7-digit entry code number. "While this code may remain unchanged for many months, the user may append his own password of up to eight characters and change it any any time,"

Booth said. The user, once his code has been accepted by the computer, may then use the machine to perform mathematical functions or to store and then execute a user-made program.

"The most important point to note is that when a function is written it can be locked so that no one, not even the function designer or the console operator, can see how the program works, or can change it. It can never be unlocked. It can only be erased," Booth pointed out. "Not only can the user protect his account number and the contents of his programs but also units of storage called workspaces", he added. "Should the need arise to store a security program before it is finally locked, it can be stored in a workspace which itself is protected by a password of up to eight letters.

"The degree of security employed is in the hands of the user, which is important because security usually costs money in both user's time and computer costs."

Despite these reassuring remarks from Pearson, Booth and Goodfellow, there was considerable uneasiness among conference participants about the security of computer systems, particularly in systems that do or will contain personal information about individuals.

J.S. Crowson of the Department of Communications argued that "the computer is only as good as the system that operates it". Citing the experience of the Canada Post Office in devising money order systems, he claimed, "People may devise many wonderful systems and for a short while they confound the crooks. But it isn't very long before the professional thieves find a way to beat the system".

Another participant who questioned the efficiency of existing security procedures was Dr. Ware, who said simply: "Nobody knows the kind of threats that will be mounted against data banks. This makes it awkward for the designer of safeguards".

Another security problem arises from the possibility of sabotage. The matter was raised in a question by Prof. Jean Baetz of the University of Montreal. "I would like to know how vulnerable in the present state of affairs are data banks on computers and communications systems - their vulnerability if a substantial segment of people from whom information is sought wished to fool the system. For instance, they could deliberately lie. Suppose a question is asked and you are supposed to reply in one way or another and you reply both ways".

To which Ware said: "I can give you an answer to that question but it won't be a useful answer. The answer is they're terribly vulnerable. But the reason it's not a useful answer is that nobody has really put his mind to trying to figure out how to protect against that kind of mischief. You can invent schemes which give partial protection. For example, suppose you answer a questionnaire for me and you misstate your salary because you think I'm being too nosy. From looking at enough people who I believe are answering honestly, one can get insight into who is misstating the facts". B. B. Goodfellow added his view that systems suffer from "medium vulnerability" to illegal access. "The real problem is that there isn't that great an urgency exhibited to do anything with it. I think we have a lot of ideas of how we could if we had that need".(1)

---

(1) A comprehensive pamphlet, titled The Considerations of Data Security in a Computer Environment, published by International Business Machines Corp., provides additional discussion of security problems.

CHAPTER IV

PROPOSALS FOR ACTION

> "We've seen the offering by various technological specialists in the computer industry of a new world with new possibilities - I hesitate to say brave new world - with many advantages through the use of computers. But many of the offerers are concerned about regulation on the basis of privacy with the apprehension that this will lead to regulation of freedom of speech. I think this is an instance of what Professor Moffat Hancock called the "transplanted category" in which by using a concept developed in one context in a completely different context for which it was not intended, you can give a spurious conclusion certain plausible effect. We should not confuse freedom of speech with the activities of the data manipulators. If we avoid regulation of the new world, the manipulators of information take over under the rubric of freedom of speech. Don't confuse this activity - a controlling activity - with freedom of speech."
>
> - E. F. Ryan
> Ontario Law Reform Commission

Much of the commentary and many of the opinions expressed at the conference suffered from the "transplanted category". The result was, of course, misunderstanding and perhaps, at times, animosity because of a lack of a mutually understood and accepted context. Therefore, before proceeding to examine in detail the various proposals for action, it is worthwhile to review some of the major areas of consensus, either declared or implicit, arising from previous chapters. This will serve as a context for the proposals.

Privacy, a concept not explicitly accepted either socially or in the law, was seen to be an indispensable element of an individual's sense of dignity. And the ability of an individual to preserve his sense of

dignity is vital to the fabric of a democratic society. An individual's privacy, defined perhaps as the desire to be left alone, is constructed on two pillars - the freedom from unwarranted intrusions upon solitude and the freedom from unwarranted manipulation, either threatened or pursued, by those in possession of the means of manipulation. Against the individual's claim to privacy must be weighed the legitimate requirements of the society - maintenance of law and order, operation of the economy, advancement of informed legislation, etc.

Information can be an extremely powerful commodity. Those who are aware of this, many of whom have legitimate requirements for information, often seek information from and about individuals. Individual privacy or dignity may be offended by this process. It may also be offended through the ways in which those who gather information then use it. The power of information is proportional to, among other things, the ability to store, retrieve and analyze it and to correlate it with other information. The harnessing of computer-communications systems to the tasks of storing and manipulating information has incomparably increased the ability to perform these functions. Insofar as these tools exist and are economically feasible, it should be assumed that many information system operators will find it in their interest to use them. A parallel requirement arises therefore, to protect the individual's interest from more intensive privacy invasions that could result if and when certain information system operators come to possess, or control, more powerful bases of information.

Using this general context, the various proposals for action can be divided into two general categories: those designed to protect directly the individual's right to privacy and those designed to circumscribe the

activities of certain operators and users of information systems and the systems themselves. These two categories, of course, reflect two legal approaches to the problems posed by information systems in relation to privacy; the one investing the individual with a right and the other specifically limiting the actions of certain agencies. In seeking to protect an individual's privacy, proposals were made that aimed either at limiting invasions of privacy or at insuring the individual's right of access to information about him held by others. Some participants emphasized the need to regulate the information systems themselves and others saw a need to regulate the actions of both the operators and the users of information systems.

Whichever of these approaches are pursued, the drafters of safeguards should bear in mind Dr. Willis Ware's warning.

> "From the individual's point of view, safeguards have to be credible. They have to look to him as though they're realistic and will, in fact, do as claimed on his behalf, and they have to be understandable. For the lay public, legislation that says a computer must have 'memory protect' and 'privileged mode' and this, that and the other technical feature that some ingenious man has discovered is wrong. First of all, legislation of that kind would be so specific that it's easy to circumvent. It's like the patent business; you can always find a way to get around it. But worse, the general public will not and cannot understand it and therefore it will not be a reassurance. The problem will not have been put to bed."

Rules or regulations have not only to be comprehensible and credible, they should be able to accommodate the inevitable changes brought about by technological advance. Professor Thomas McPhail, supported by Dr. VanderNoot, also pleaded for consideration of the special and increasingly important role of social science research.

"Proponents of legislation severely limiting the rights of researchers", said McPhail, "have to consider the possible spin-offs of legislation. In an era where accelerated change, shifts in living styles and escalation of 'deviant' behavior is the rule, social statistics become almost mandatory if governments and private agencies are to have some yardstick to gauge present programs and, more important, what future societal trends and programs will be like."

1. A Right of Privacy

To protect privacy, one must begin with a definition of the quality to be defended. Attempts usually begin with Article 12 of the United Nations' Universal Declaration of Human Rights.

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

By itself, this is of little help in deciding what privacy is. Another suggestion is that privacy is the right "to be left alone". As formulated, such a concept appears to cover at least the major dangers to privacy presented by information systems; i.e., the threat of probes into an individual's activities and the threat posed by those who would use information systems to manipulate individuals. Recall Allan Gotlieb's concept of privacy as the right to disconnect:

> "In the privacy domain, there may be found the desire to be left alone, to be left in peace by the rest of the community, which means the availability of sufficient space to provide protection from the static of one's neighbours, to die alone if one so wished, to rest outside of society, to be non-productive,

> to be off-beat, to be an alien, if one so desired, to turn off the connection. It may also involve respect for one's anonymity in a public place. It may involve being able to establish intimate relationships with others on the understanding that whatever passes between those concerned will not be made public."

Gotlieb also implies that a right to know or freedom of information is a vital prerequisite to the establishing of a right of privacy.

"To what extent is it practicable and feasible to protect the privacy of the individual in a society that looks and behaves more and more like a glorified information system?" he asks. And he cites the spectre of information being held and manipulated by fewer and fewer highly skilled people."

"This increases the danger that the gap between the administrators and the rest of society may widen. The individual may come to feel to an ever increasing extent that he is spied-on in an information-dominated society."

Justice Minister Turner appears to agree for he said: "The rights to privacy and freedom of information are not contradictory but complementary; the right to privacy and the right to know are the twin freedoms indigenous to, and necessary for, the creation of a democratic order."

No matter how these rights are articulated, the real problem is interpreting and enforcing them in specific cases. Willis Ware, for one, seemed content to have an individual's claim to privacy, in the face of conflicting claims, adjudicated by the courts.

> "Suppose a data bank exists and some of that information is used and I don't like it. I sue.

> If I win the case, there is precedent for what is in the individual's best interest and all other operators of data banks take notice. If I lose the case, then I as an individual have to conclude that that class of information has been decided collectively by society and by the legal processes of society to be necessary for the general welfare and benefit of the society. And I must yield."

Unfortunately, this is probably too simple a view. Conference participants raised many questions about how such a right would work. Should for example, there be an "offence" of invasion of privacy and/or a "tort" of invasion of privacy with appropriate remedies, to whom should the right of privacy extend? One workshop pondered how to create a right to privacy for individuals without also passing on that right to corporations or governments. Also, it was recognized by many that invasions of privacy are more likely to create psychological damages than physical damages and that compensation for psychological damages is, to say the least, a hazy legal procedure.

H. Allan Leal of the Ontario Law Reform Commission insisted, however, on the importance of compensating the person who has been damnified. "I'm aware that Westin believes the action for damages is too blunt an instrument to apply where someone has been damnified by some malfunction, personal, mechanical or otherwise. But I think that in addition to your regulatory procedures, standards and penal sanction, this is how you get to the cutting edge of the injury". He was supported by Parkhill, among others, who called for the right to sue for damages if privacy is breached.

Perhaps the most coherent explanation of the inadequacies of establishing a right of privacy was given in a 1968 Report on Protection of

Privacy carried out for the Ontario Law Reform Commission. The report indeed proposed the establishment of both an offence and a tort of privacy but it also argued that, while helpful, these still would not provide adequate protection for the individual.

> "The protection of privacy poses major problems of a social, psychological, economic and ethical nature which are simply non-responsive to attempts to deal with them either in terms of pre-existing legal categories or in any fashion that falls short of being fully comprehensive. If the objective is to grant protection to privacy that is reasonable under the circumstances of any given case, then legislation must not only limit the claim to privacy by this formula, but should also limit those competing claims that are based upon considerations of public interest, economic well-being, commercial expedience, control of anti-social activities and all the rest. Without creating parallel norms, particularly in those areas with either a strong laissez-faire tradition or an established set of distinctive institutional values, then the exceptions inherent in granting protection to privacy that is "reasonable under all the circumstances" may eat up the rule. Loss of privacy, and the resulting decline in the quality of our lives, is really the by-product of hundreds of well-intentioned attempts to come to grips with the major problems of our modern urban-industrial society using advances in technology and streamlined commercial practices to achieve this with a minimum expenditure of time, effort and resources. Controls prompted by the apprehension that the whole of these attempts is unreasonable, but the effectiveness of which depend solely upon a determination of whether any constituent part thereof is by itself unreasonable, appear to the writer to be foredoomed. If we are concerned with the jeopardization of the quality of life, then the scope of our future actions must equal the scope of that which is at stake. The creation of broad spectrum limitations upon the means and the interests that threaten this quality is in fact the substance of the protection of privacy; the mere articulation of a right to privacy, with nothing more, is simply its shadow."

While the Ontario Law Reform Commission argues here that

establishment of a right of privacy might not do much good, many conference participants insisted that it could do a lot of harm, particularly if it went so far as to limit freedom of speech or the right to know. Hugh Lawford of Queen's University, for example, argued that "no legislation should be enacted to protect privacy without legislation to protect freedom of information." And most participants appeared to agree with him. Here is the consensus recorded in the conference summary report:

> "There was almost complete agreement, expressed in ten of the workshops, that there is a need for freedom of access to information. This was regarded as being particularly important with respect to government information. And a Freedom of Information Act, similar to that in effect in the United States, was considered by many to be necessary."

Although the specific question did not arise at the conference, it is worth considering whether a right to information is implicit in a right to privacy. In other words, if it is assumed that part of the right to privacy is the right to "liberate" sensitive personal information held by others, then perhaps an individual could claim damages against an agency attempting to withhold such information in order to blackmail him. Allan Gotlieb, as indicated above, certainly considers this freedom from manipulation to be a vital pre-requisite to privacy. But he also suspects that "the law is powerless to prevent the expanding gap between those who manipulate information and those about whom information is being manipulated."

Whether or not freedom of information is considered an integral component of a right to privacy or a separate right in itself, the same series of questions posed by the Ontario Law Reform Commission above with respect to privacy could apply to it as well. Would the establishment of

a right of privacy or a right of information be adequate to protect against damages done by others exercising legitimate, conflicting rights? In any event, it is likely that Canada will opt for separate legislation to protect the public's right to know. Both Professor Lawford and Justice Minister Turner cited other reasons, not directly related to the privacy consideration, to warrant bringing forth a law to ensure the individual's right to information. Prime among these, it will be recalled, is the idea that citizens need access to government documents in order to play a meaningful role in the process of democratic government. And Justice Minister Turner spoke strongly in favor of the introduction of a Freedom of Information Act.

> "What is necessary is a Freedom of Information Act entitling the individual to information which the government authority has arbitrarily seen fit to withhold. Indeed, as Professor Lawford has pointed out, the Canadian Government has yet to enact a law respecting clearance of, and access to, Government documents. The situation both in respect of access to documents in the national archives as governed by the Public Archives Act, as well as documents still in the possession of government departments, is far from satisfactory. It is true that certain classes of government information may not be disclosed; but the criteria for non-disclosure should be set forth publicly in the statute, this in itself constituting a kind of information about what information is not available; or the right of the public to at least know on what grounds and under what circumstances it may not know. For example, the Freedom of Information Act passed by the U.S. Congress in 1966 and designed to make executive records more accessible to the public, set up eight categories of sensitive information to be exempt from disclosures. These included, inter alia, matters such as defence or foreign policy secrets authorized to be kept secret by executive order, etc.
>
> But perhaps the most interesting exemption is that of personnel, medical and similar matters, the

> disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Indeed, the important point about the Freedom of Information Act, and one not entirely appreciated, is that the right to privacy is as much a goal of the Act as the public right to know. For the Act was to provide a basis for safeguarding from disclosure private information about citizens that the government had acquired. The two rights, then, are not contradictory but complementary; they are companion rather than conflicting freedoms; the right to privacy and the right to know are the twin freedoms indigenous to, and necessary for, the creation of a democratic order."

If one is to accept the arguments of the Ontario Law Reform Commission and many others, the relatively simple act of creating individual rights to privacy and freedom of information will not be adequate to protect citizens from privacy invasions in the modern, industrial, urban state. In addition, laws appear necessary to circumscribe the activities of many agencies, individuals and devices that may, accidentally or intentionally, invade personal privacy. A list of such potential invadors would have to include those interested in wiretapping, surveillance devices and so on. The orbit of the Queen's conference, however, was restricted to the field of computers, information systems and the activities of information system operators and users. But that action must be taken on them too was widely recognized. As J. M. Sharp, a panellist and Professor of Law at the University of Manitoba, explained: "There can be no confident self-regulation of input, storage and outflow of data, and the best goodwill in the world of the operators of data banks cannot guarantee security of privacy without legal sanctions to lend 'teeth' to the good intentions."(1)

(1) Sharp's position paper, in effect a detailed blueprint for legislative action, is reproduced in full as Appendix VI.

2. Curbing Misuse and Abuse of Information Systems

> "My concern is that in attempting to regulate the present problems we will develop rules of such generality that we will interfere with systems of the future that aren't subject to these same dangers."
>
> - Hugh Lawford

> "In laying down the rules of the road before the road is used, we can avoid some serious collisions."
>
> - A. E. Gotlieb

As perhaps in any discussion about potential legislative action to curb the activities of certain people and agencies, there were hawks and doves. And the color of one's plumage, as it were, seemed to depend on the extent to which one was afraid that legal measures could interfere with technological development. The dilemma often took on a devastatingly Swiftian air. Lurking behind the apparently calm, reasoned positions of both those who called for broad protective legislation now and those who cautioned against meddling with technology were the implied threats of chaos. And the middle road of common sense, if indeed there is such a road, appeared to be more like a tightrope than a road, upon which it is difficult to stand and even more difficult to stay for any length of time.

B. B. Goodfellow of IBM Canada Ltd. expressed concern at the prospect of "excessive legislation on one narrow element of a broad problem. Standardization inhibits innovation". He was supported by at least one workshop which reported: "There is a real danger in trying to be too broad or sweeping initially. This would almost certainly be interpreted in ways which would inhibit or delay advancement of technology."

For the "hawks", Dr. Willis Ware argued: "I would rather not have data banks become the problem that pollution has become. Thus, my view is that we should vigorously and aggressively formulate appropriate safeguards, mechanisms and legislation. Let's try to be ahead of the situation before it is too late."

Again, the problem of context (or lack of it) is probably largely to blame for this apparent polarization of opinion. It is possible that legislation or regulations can be devised that will adequately protect the public without inhibiting technological innovations. Indeed, it will probably be more difficult to convince people that this can be done than to actually do it.

Take, for example, the simpler of the two aspects of the challenge information systems present; that is, ensuring that the personnel involved are reputable, honest, technically competent, etc. One might expect to find a sharp division of opinion between information system operators and planners as to the need for government action here. In fact, no one denied the need for action. There was some debate on the best way of assuring personnel quality but none on the principle. As Dr. Willis Ware put it: "I want some protection against the possibility that the (operator) is not as honest or careful as I thought he was. I want some legal recourse."

In the debate, Mers Kutt, former president of the Canadian Information Processing Society and Thomas McPhail of Loyola University pleaded the case for self-policing by professional groups.

Kutt, speaking on behalf of computer professionals, said, "the first thing that computer societies should do is educate their members on the

sensitivity of the problem and the rights of the individual to prevent, among other things, the innocent misuse of files. The second thing societies should do is establish professional standards and a code of ethics for computer people involved in information handling activities."

Professor Thomas McPhail, advancing the position of social scientists, suggested that "perhaps the most fundamental (solution) is not to be found in legislation but rather is to be found in the setting of high professional standards for entrance into various social science research disciplines. A practical result of this would be the adoption of some type of code or statement of scientific ethics to be adopted by the various learned societies in Canada." But McPhail also encouraged government action to give teeth to professional ethics. "There are in North America roughly 40,000 social scientists", he said, "it only takes a few who abuse ethical standards to give the profession a bad name."

Those advocating government action were split on how that action should be taken. D. F. Parkhill of the Department of Communications and J. M. Sharp of the University of Manitoba argued that all employees of information system operators should be licensed and bonded. This appeared to have the support of most participants of the conference and there was little discussion one way or another. One thoughtful alternative, however, was presented by John Russell of Systems Dimensions Ltd., Ottawa.

> "Legislators and computer experts alike acknowledge the need to reassure the public of the integrity of the technical insiders who could conceivably gain privileged access to their private files. Towards this end, it has been proposed that computer personnel form a professional association to which a government could delegate regulating responsibilities similar to those delegated to the medical, bar and chartered accountants associations.

> Such an association might be charged with two major responsibilities. The first might be that of establishing professional standards sufficient to inspire public confidence in the capability of data bank systems engineers to build in adequate security controls. The second might be that of maintaining security by controlling employment in the field.
>
> A regulatory association capable of assuming these responsibilities would take many years to mature to a point of effectiveness. In an environment requiring rapid and continuous adaptation to new technology, one might wonder if such an association could ever catch up with the arts and skills being developed by its members.
>
> Since, in the minds of the public, the issue would be one of security rather than professionalism, I would submit that the public interest would be more effectively served through the use of conventional check-outs for the personnel involved. The just application of employability criteria similar to those presently in use in sensitive government and industrial activities should suffice to ensure adequate confidentiality of information."

Proposals of ways to control the information systems themselves were both more numerous and more contentious. Professor J. M. Sharp, for example, suggested that "every data bank should be subject to a licensing requirement regardless of whether it is operated by a government agency, insurance, finance or credit reporting company or other person." Others even suggested that certain kinds of data banks should be outlawed. Obviously wearied by it all, one participant, himself a data bank operator, was nevertheless able to see a bright side. Ian Sharp, president of I.P.Sharp Associates Ltd., Toronto, rose at the end of the final plenary session to comment:

> "With the possibility of Finance Minister Benson's White Paper being translated into law, there could be set up a data bank containing so much information regarding the assets of all individuals in Canada in one form or another that I would like to suggest that any legislation should be phrased in such a way as to make the implementation of such a data bank illegal."

Exactly which data banks should exist and which should be regulated was never settled. One workshop reported "some agreement" that only those data banks containing information "that can potentially harm people" should be regulated. The conference summary report says that "all levels of personal data banks should be licensed but that the degree of licence would vary with the classification of the information contained."

Having established through some means, such as Professor C. C. Gotlieb's classification system, which information systems require surveillance in the public interest, the next problem is to discover how to provide a useful, adequate and credible surveillance. Again, Dr. Willis Ware provides a full list of the information he would want to have on data bank operations, were he a regulator.

> "Before an owner and operator of a data bank could be licensed, so to speak, I would ask that he demonstrate to an appropriate regulatory body such things as the following:
>
> * the nature and purposes of his data bank; the use to which the data will be put; and the general class of customers it will serve,
>
> * precise identification and description of the data sources on which it will draw, and the checks that will be applied to validate the information from the sources,
>
> * a complete description of the safeguards of the system (physical, hardware, software, communication, personnel and administrative/management) that protect information and control its divulgence,
>
> * a complete description of the procedural safeguards (software or manual) to edit source information for errors, to assure posting information to correct dossiers, to resolve ambiguity in identification of an individual, to treat information of doubtful validity and to establish confidence levels on information derived or inferred from fragmentary data,

* a complete description of the audit processes incorporated in the system, and the audit information that will be made available for periodic review,

* the mechanism whereby an individual can review his dossier and the sources from which the dossier was compiled, and challenge its contents and correct errors,

* the tests and inspections that he has performed on the system to assure that it does operate properly, and especially that the software has been verified completely designed."

Ware also explained why data bank operators should be obliged to fulfill these requirements, requirements that he willingly admits are stringent. "I would rather begin too strongly", he said, "and weaken controls as experience shows it possible than recover from awkward oversights after the fact." Some of his suggested requirements, such as means of validating source data and security measures taken in and around the data bank are obviously important but others, although less obvious, could be equally important.

Consider for example, some potential problems that can arise with users. Ware argued that the operator must accept prime responsibility for certifying that his users are as they represent themselves and to keep others out. Then, "the provisions of communications' secrecy acts would seem to be applicable since users will receive information as a privileged communiqué and should therefore be liable for willful or negligent transfer to other parties."

If one of the users is another data bank, Ware would call for additional safeguards on the operator's part. "Audit trails must be maintained so that he knows where copies of any or all parts of data exist in computer files, and he must accept responsibility for updating or correcting such copies promptly and responsively. Conversely, if he receives data from another data

bank, he must keep audit information so that original sources can be identified at a later date. This could be crucial in the event of damage suits in which the operator's liability should be shared with data sources." Willis Ware argued that the existing societal process of legislation as interpreted by the courts can function to establish the precise details of an individual's claim to privacy.

Once a regulatory authority has established the kind of information it needs in order to perform its function, it must then establish sets of minimum requirements for various categories of data bank operations to meet and penalties to impose in cases of failure to meet them. To judge from the conference discussions, people are particularly concerned, even anxious about the data gathering, verifying and distributing functions of some data bank operations. Professor J. M. Sharp, for example, explored some of the dangers that can arise in linking two data banks and called for "close scrutiny" of this practice.

> "The greatest importance of this type of scrutiny would be in relation to data banks with international links. It has been suggested, and the writer concurs, that the total effect of a drain of personal, commercial and even governmental data from Canada to foreign countries could be the creation of a serious threat to the Canadian economy, and a violation of Canadian sovereignty none the less real by reason of the fact that it is an intangible, "invisible" violation.
>
> Regulation of inter-memory bank links between provinces is only fractionally less crucial, for the entirety of the data in one bank which has drawn on many sources takes on a manifestly greater significance than the sum of the contributions of the various original constituent sources.
>
> Even <u>within</u> provinces, particularly the larger, more "commercialized" ones, the same problem arises; an intra-provincially linked, but not externally-linked, system should be subjected to provincial regulations along similar lines. Here, again, the need for uniform provincial legislation is apparent.

> The related topic of sales of information by data bank operators must be considered. A recent press report states that a U.S. data system went out of business and proceeded to sell dossiers on three million individuals, as a company asset, to the highest bidders. It is scandalous that information, perhaps volunteered by an individual for a specific, limited purpose, and perhaps of a highly confidential nature, should find its way into the public market to be hawked around as if it were clearance stock.
>
> It is strongly suggested that the dual type of links between data banks, and output therefrom, should be regulated closely, even, perhaps, to the extent of legislating some new concept of "qualified property" in both the physical computer tapes, cards, etc., and in the intangible information which stems from these sources. The existing case law in this area is at present inadequate and is unlikely to develop either quickly or fully through new judicial decisions."

Claude-Armand Sheppard argued in his position paper that "data furnished by citizens to any government department or official agency at any level should not be available to any other department or agency at any level or to any outside source". He also would simply forbid the constitution of large pools of data either in government or in private hands and would "prohibit the recording in data banks, except for purely statistical purposes, of any reference to, or indications of, an individual's ethnic origin, religious beliefs or political opinions."

Parkhill demanded "recognition that the individual named in a file is the ultimate owner of that file and, consequently, has the sole right to determine the persons to whom access is to be granted." He also suggested improperly authorized access to an individual's file should be a serious crime punishable under the criminal code by severe penalties.

As for collection and verification of data, one finds proposals for

elaborate mechanisms for people to be able to check personal information held in data banks, for forbidding storage of unverified information obtained by interviewing neighbors and for establishing cut-off dates in advance for certain types of information.

Parkhill suggested that it should be "the responsibility of the data bank organization to provide each individual named in that bank with a monthly statement of the contents of his file, the names of those people and organizations who have been granted access and the purpose and authority for such access." A clause to this effect is also contained in Tim Reid's data bank bill before the Ontario legislature.

Parkhill also suggested that "every person have the right to inspect his file at any time, to question its contents and, where disputes arise, to order the offending entries deleted until such time as the data bank operator can demonstrate their accuracy before an independent tribunal."

The point of the right to review was also mentioned in several workshop reports, indicating that this is a major area of grievance.

Professor Sharp acknowledged, however, some restrictions on this proposed right. "The process could be expensive; in this case, charge the individual a realistic fee. This would not only avoid undue expense to the operator, but also deter frivolous or spurious requests."

Pearson of the Associated Credit Bureaus of Canada vigorously opposed the suggestion that data bank operators should send a print-out to each individual on a monthly basis reporting uses of his file. He claimed the U.S. government had backed away from installing such a requirement,

realizing that it would be prohibitively expensive. One workshop noted that "no regular reporting should be necessary since the individual should have access to his file and he knows that the file exists at a specific location." But another workshop cautioned that "there might be 'inequalities of access' due to individuals' differing economic situations." Pearson also claimed that most people don't want to see their credit record because they know it is good and they don't want the information flowing through the mails.

One reason for the high degree of accuracy of information held by private agencies, such as credit bureaus, advanced by one participant is the existence of competition. There is a natural check on accuracy, he said, when the information selling business is competitive. He suggested that greater attention should be paid to scrutinizing situations in which no competition exists.

Professor Sharp argued that cut-off dates should apply to certain facts stored in information systems after the lapse of pre-established periods of time. And he noted the practice of the Associated Credit Bureaus Inc. of Houston, Texas of not reporting bankruptcies longer than 14 years from the date of adjudication of the most recent bankruptcy nor recording accounts placed for collection longer than seven years. "While it may be argued", Sharp said, "that cut-off dates should not be applied to certain governmental data banks (e.g. any data bank or portion of memory bank controlled by the Dominion Bureau of Statistics which would separate identities and information before public release), it has been widely accepted that, in the interests of protecting privacy and with no substantial impairment of freedom of information, cut-off dates should apply to certain facts after the lapse of given periods of time."

To expedite the process, Ware suggests that "the individual probably should have a legal, court-created document certifying that some action has been taken. Consider the person who has been arrested and accused of a felony," he said. "Later, however, he is acquitted. This fact may well find its way into his credit reference file and he should have some positive confirmation from the data bank that his arrest experience has been expunged from all copies of his credit file." (1)

Finally, both B. B. Goodfellow and John M. Russell offered potential law - or regulation-markers some technical advice. Goodfellow observed that:

> "There is less security consideration on defence systems - and needs to be - than there is on other systems. And the reason for this is that defence systems are so protected by a host of other things like the surveillance of all the people and barbed wire fences and the like. You actually should, and in most cases they do, build more security into, for example, one of the state's Blue Cross data banks than they would into some of the defence systems."

Still on security questions, John Russell pointed out that the administration of passwords and other authorizing instruments is a costly and time-consuming function which cannot be hurried. "Draftsmen of legislation should therefore provide adequate statutory time delays between the application and the granting of authority to access a data bank."

3. Vehicles of Action

The most common suggestion was to establish a regulatory agency with responsibility for information systems of specified types and provide it with

(1) There is a self-defeating feature in this proposal - that is, the data bank, for its own protection, would have to keep a record of its "positive confirmation" to the person.

licensing powers. There was little discussion as to whether the same agency might have powers over both information systems and their operators or whether there should be two agencies. There was, however, considerable emphasis on the necessity for government-operated information systems - some would even include police files - to be subject to the scrutiny of the regulatory authority. Some doubted this would work. "How can we expect one government agency to provide impartial and credible surveillance over another?", one participant asked rhetorically. There are, of course, several instances of this happening in Canada, but perhaps they provoked the remark!

An argument against licensing (although not against government regulation) was presented by A. E. Ende of the U.S. Federal Communications Commission in one of the workshop sessions. He argued instead in favor of setting standards and policing them. He said that licensing tends to be based on criteria taken from past experience which may no longer be relevant. Once embedded, however, these criteria are difficult to throw out. Also, licensees become very tenacious about their licences, he argued. By establishing standards only, these can be modified as required and published. Anyone who doesn't meet the standards is punished. Finally, Ende pointed out that licensing is perhaps a useful tool where a government is awarding franchises for the use of limited resources (e.g. broadcasting frequencies) but this does not apply in the case of data banks.

In addition, the idea of setting up a body to oversee the regulation process was extremely popular. Six of the workshop groups discussed the possibility of establishing an office of an ombudsman or a commission or tribunal with limited authority. Its function would be to recommend appropriate

regulation or legislation but it would have neither regulatory nor legislative powers. It could also hear cases of specific injuries resulting from information systems, conduct research into data bank developments, recommend data classifications, review professional standards, etc. Proposals like this appear to represent the general feeling of a need for an advisory body at arm's length from any regulatory or legislative authority. Some people, for example, suggested it should include representatives from various groups in both the private and public sectors.

4. A Note on Legislative Competence

Professor J. M. Sharp argued the case for federal jurisdiction over information systems, mainly on the following grounds. "I can envisage nothing more unsavory or undesirable than that a given province should become the Las Vegas of the computing industry because, while the others have regulated, this one attracts the Panama flag of convenience of the computer industry. And this I think could quite easily happen unless we have a federal assumption of jurisdiction."

In Sharp's view, "at least those computers and data banks which participate in inter-provincial or international flows of credit,commercial or other information would seem to be pre-eminent candidates for federal legislation."

For constitutional support, he referred to the "stream of commerce" doctrine, the telecommunications analogy as expressed in the Telesat Canada Act, 1969, and the criminal law and national security. He admits, however, that for intra-provincial systems, "provincial legislation (ideally in the

form of a uniform statute) would be needed. Perhaps a rather loose analogy could be drawn from the inter-relation of the federal Narcotic Control Act and Food and Drugs Act on the one hand and the provincial Pharmaceutical Acts on the other hand. To some extent these are complementary; there is no reason why an interlocking system of federal-provincial legislation should not be evolved to deal with data banks and the information they store."

Professor Douglas A. Schmeiser of the University of Saskatchewan College of Law and Chairman of the panel session on legal and regulatory means of reaching objectives, finds "the arguments in favor of federal jurisdiction over the basic area of privacy are not really very compelling." But neither he nor Claude-Armand Sheppard, who agrees with him, elaborated on their views.

Sheppard did say, however, that "the constitutional aspects of legal controls over data banks are not as intricate as they might appear. It seems highly doubtful to me that the federal government could lay claim to exclusive jurisdiction. In all probability, and in the good old schizophrenic Canadian tradition, jurisdiction is shared between Ottawa and the provinces."

5. International Considerations

In some senses, the argument over legislative competence within Canada may be a meaningless exercise, for it was recognized at the conference that the "Las Vegas" of the Canadian data bank business could well be Las Vegas itself. Because of the numerous, open telecommunications circuits connecting Canada and the U.S., it is virtually impossible to stop a data flow across the border if data bank operators want to organize their affairs

in that direction. Canadian laws may insist that data on Canadians be stored in Canada, as some conference participants urged, but it would appear difficult to stop anyone determined to store copies of that data in the U.S. if he wished to do so.

Therefore, as others suggested, notably Guy Braibant of the French Conseil d'Etat, avenues of international co-operation should be explored. As Braibant put it: "If certain countries adopt severe legislation and others do not, with the developments in data communications we run the risk of having data bank havens in certain countries. I think that during the next decade the United Nations without doubt will have to study the creation of international agreements in this area as it has done in the area of telecommunications."

International action does not, of course, obviate the need for domestic action. If Canada doesn't take action internally, regardless of the success of international negotiations, the country could well become one of the data bank havens Braibant speaks of!

6. Conclusion

Seven of the twelve workshop reports call for the establishment of a task force to begin studying possible legislative action. Some called for a federal-provincial study group, others wanted representation on the tak force from the public and private sectors. One even eschewed the idea of a task force in favor of "a small, working group" to study carefully the many questions raised at the conference.

Perhaps these proposals are the best measure of the extent of the

belief that action is urgently required. And that would appear to reflect agreement with A. E. Gotlieb when he said in his position paper:

> "The gap between technological development and legal regulation cannot be permitted to widen and must quickly and decisively begin to close. Government at the federal, provincial and municipal levels, law associations, universities, scientists, scholars and all concerned individuals have the responsibility to propose solutions designed to recognize and protect the needs of the individual in the new society which the computer and telecommunications promise to bring about."

APPENDIX "A"

Definition of Privacy

All workshops discussed the concept of privacy, except one which did not do so explicitly. Almost unanimous agreement was reached to the effect that privacy should receive increased protection, although not necessarily on an unconditional basis.

Most workshops had difficulty in trying to define the concept of privacy and several referred to the necessity of elucidating the notion of privacy as a legal concept, or indeed to elaborate on a philosophy of privacy. Some workshops doubted that this could be done except on an ad-hoc basis and others felt the concept varied with the historical or social circumstances and should be left to the courts.

Again, others reached the conclusion, that the right to privacy should be expressed in the law and that it should be in accordance with the Universal Declaration of Human Rights.

There was a marked difference of opinion on the questions whether computers were relevant to the issue of privacy. Some thought that computers have a direct impact on privacy -- others that computers have nothing to do with privacy of freedom and others that computers are relevant to the extent that they magnify the problem.

Finally, the opinion was expressed that privacy should not be confined to computer-based systems.

Freedom of Access of Information

The right to privacy has to be balanced by two other requirements. It was generally recognized that there <u>were</u> needs for data banks arising out of the needs for planning, research and commerce.

Further there was almost complete agreement, expressed in ten of the workshops, that there is a need for freedom of access to information. This was regarded as being particularly important with respect to government information, and a Freedom of Information Act, similar to that in effect in the United States, was considered by many to be necessary.

Technical Aspects - Impact of Computers on Privacy

There was a division of opinion as to whether or not computers had a direct relationship to invasion of privacy. The predominant opinion was that the computer by permitting faster searching of more comprehensive files has indeed changed the quality of the privacy problem. The computer, however, does present the possibility of implementing more effective security controls than possible in a manual system.

Although some papers implied a high degree of security in multi-user communications oriented computer utilities, it was felt that the state-of-the-art was not adequate to handled such systems. The level of security protection needs to be appropriate to the type of data in a data bank, and this might be best achieved by using separate systems for different types of data banks. Aside from the security problem, it is not regarded as presently technically feasible to implement a national data bank on a single system. A network of computers might be possible for the purpose.

Task Force

Seven groups recommended that a task force be set up in one form or another. Three refer specifically to a Federal-Provincial Task Force, while one suggests representation by lawyers, computer

specialists, social scientists, business, government and education. Suggestions for its tasks include a review of present practices and laws, a survey of current levels of dissemination of personal data, the identification of specific areas of concern, a definition for concepts such as privacy, data banks and information systems, a study of the constitutional issues and the recommendation of guidelines and new legislation. A number of groups stressed that such a task force should be set up as soon as possible.

Commission-Tribunal-Ombudsman

This concept, in varied forms, was mentioned by six workshops. The body would have neither regulatory nor legislative powers but could recommend appropriate regulation or legislation.

Some suggested functions:

-- consider specific injuries from misuse of information
-- advise on potential data bank development; conduct research into data classifications
-- adjudicate complaints
-- establish professional standards; examine types of information being stored and uses to which it is being put
-- license data banks; require periodic reports on systems procedures by operators; require prior approval for interchange or collation of information between different systems.

Proposals made for both federal and provincial ombudsmen. Suggested Commission or Tribunal should be fed-prov, include reps from industry (one proposal that majority of members be from private sector), universities and groups such as civil liberties and consumer associations. Note: The Commission or Tribunal is also seen as an interim measure toward legislation, as a substitute for it, or as an adjunct to a Task Force Investigation.

Professional Licensing and Registration

Almost all workshop groups recommended that some form of licensing and registration was required. This requirement was necessary for control purposes and not for the sake of licensing per-se. Licensing should identify the type of data bank and should be administered by an independent body. It was suggested that all levels of personal data banks should be licensed but that the degree of license would vary with respect to the classification of the information contained. In this regard it was noted that a person could be identified even though his name did not appear in the record.

One workshop suggested that licensing of data banks, that were remotely accessed, was necessary, as the security problems, associated with time sharing have not yet been solved.

Another workshop posed the following questions:

- is licensing desirable?
- who should be licensed - investigators
  - owners of data banks
  - programmers?

In general people should be licensed for ethical activity.

Legislation and Regulations

Four workshops made no specific suggestions for legislation, although the fact of their being legislation in respect of privacy was assumed by one of the workshops to the extent of establishing a regulatory authority at least.

Seven workshops made specific suggestions for legislation of the "Bikini" type, as defined in one workshop, that is legislation to cover the essential points. These essential points appeared to be among the following:

a. the protection of the privacy of individuals (6 out of the 7).

b. this protection was by way of establishing a civil liability for damages in three cases, while a criminal liability was inferred from the suggestion of one workshop, in addition to a civil remedy.

c. a right of privacy to be provided in accord with the Declaration of Human Rights was suggested in two of these workshops.

d. individual's review of any file on him to be a matter of right (two workshops).

e. the access of an individual to his file to be controlled by him (two workshops).

This group had two workshops suggest that the legislation should be of the type that would permit experience to be gained from which the necessity of further legislation could be more knowledgably determined. One suggested that this essential legislation was urgent. Two workshops in this group were interested in legislation providing more freedom of access to government information.

Other matters of legislation touched upon by these groups were that legislative rules should apply equally to government files as well as to others and that the information required in the public interest should be clearly set out in legislation as well as to whom it can be released. One workshop of this group suggested that federal legislation was require because of the "haven" problem and the mobility of data.

Workshop number three dealt with legislative proposals at length, and although some of their points were covered by other workshops it is felt that its report is better referred to than summarized.

In the result all but four workshops out of twelve recommended some form of legislation. No workshop appears to have recorded opposition to legislation and one even suggested that some legislation was needed as soon as possible, but cautioned about proceeding on insufficient information.

Penalties

Eight workshops suggested that penalties should be created for misuse or negligence in the use of information. Six of them distinguished between criminal and civil penalties. In the latter case, misuse of information should give rise to action in damages.

It was also felt by one workshop that the transfer of information from one data bank to another should be prohibited. It was suggested by one other workshop that a public fund be created to indemnify personal loss where litigation is not a practical remedy.

Several comments were made about government's role as a major data gatherer.

-- not enough attention was paid to government's computerized files; that any regulatory body should be independent of government because government is the owner of such large systems; that, excluding national security, government should be subject to any controls adopted.

-- In two workshops the opinion was expressed that even police systems should be included.

International Issues

Three workshops expressed concern that legislation should ensure Canadian control of data banks especially when they contain personal information about Canadians. One group felt that avenues of international cooperation providing for the protection of individual privacy should be explored.

APPENDIX "B"

Panelists and Speakers

Panel 1

Privacy and Openness as Social and Legal Concepts

Chairman — Dr. John J. Deutsch
Principal and Vice-chancellor
Queen's University

Mr. A.E. Gotlieb
Deputy Minister
Department of Communications
Ottawa

Me Claude-Armand Sheppard
Etude Robinson, Sheppard
Drymer et Shapiro
Montréal

Hon. John Turner
Minister of Justice
Ottawa

Panel 2

Data Banks: Existing Technology and Practice

Chairman — Prof. Jacques Saint-Pierre
Directeur du Centre de Calcul
University of Montreal

Mr. R.F. Linden
Department of Industry, Trade and Commerce
Ottawa

Dr. T.J. Vander Noot
Associate Director General
Operations and Systems
Development Branch Dominion
Bureau of Statistics, Ottawa

Mr. M.T. Pearson
General Manager
Associated Credit Bureaus of Canada

Panel 3

Data Banks: Direction of Development Resulting from Needs and Technology

Chairman

Dr. Louis Robichaud
Directeur
Centre de traitement de l'information
Laval University

Mr. D.F. Parkhill
Director-General
Policy, Plans and Programs
Department of Communications, Ottawa

Mr. B.B. Goodfellow
Director
IBM Canada Laboratories

Dr. Willis H. Ware
The Rand Corporation
Santa Monica, California

Guest Speaker

Hon. Eric Kierans
Minister of Communications

Panel 4

Objectives for Securing Privacy and Freedom of Information in Data Banks

Chairman

Mr. T.B. Smith
Advisory and International
Law Section
Department of Justice, Ottawa

Prof. Calvin C. Gotlieb
Director
Institute of Computer Science
University of Toronto

Prof. Hugh Lawford
Department of Law
Queen's University

Prof. Thomas L. McPhail
Co-chairman
Department of Communications
Arts
Loyola College

Panel 5

Professional and Technical Means of Reaching Objectives

Chairman — Me Guy Houle
Services juridiques
Bell Canada

Mr. Mers Kutt
President
Consolidated Computer Services Ltd.

Mr. David F. Booth
I.P. Sharp Associates Ltd.

Mr. J.M. Russell
Vice-president
Research and Development
Systems Dimensions Ltd.

Panel 6

Legal and Regulatory Means of Reaching Objectives

Chairman — Prof. Douglas A. Schmeiser
College of Law
University of Saskatchewan

Dr. Paul Armer
Director, Computation Center
Stanford University

Me Claude Frenette
Vice-president
Power Corporation of Canada Limited

Prof. J.M. Sharp
Legal Research Institute
Faculty of Law
University of Manitoba

Final Session

Guidelines

Chairman — Me Jean Beetz
Doyen de la Faculté de Droit
University of Montreal

Rapporteurs — Yves Legris
Department of Communications

Leslie Meizi
University of Toronto

Conference Committee

Conference Chairman	Richard Gwyn Department of Communications
Programme Chairman	Calvin C. Gotlieb University of Toronto
Members	J. Ryan Department of Justice
	J. Crowson Department of Communications
	D. Booth I.P. Sharp Associates Ltd.
Arrangements Chairman	Hugh Lawford Queen's University

APPENDIX "C"

P A R T I C I P A N T S

ABBEY Dr. D.S.
Ontario Institute for Studies
in Education
Toronto

ADAMEK P.
Bank of Canada
Ottawa

ALBRECHT L.K.
Royal Insurance Group
Toronto

ALLEN R.E.
Canadian Pacific Railways
Montreal

AMEY Dr. G.X.
Defence Research Board
Ottawa

ANDERSON M.F.
Simpsons-Sears Limited
Toronto

BALMER D.
Canadian Bankers Association
Toronto

BAUDOT J.
Centre de Calcul
University of Montreal

BAXTER Dr. D.C.
Department of Supply & Services
Ottawa

BEAVIS D.B.
Privy Council Office
Ottawa

BEETZ J.
Faculté de Droit
University of Montreal

BEEZLEY J.A.
External Affairs
Ottawa

BENETEAU B.A.
Québec - Téléphone
Rimouski

BERGERON G.
Department of Communications
Ottawa

BONYUN Prof. D.A.
Computing Centre
Acadia University

BOUWMAN R.J.
B.C. Telephone Company
Vancouver

BOWKER W.
Institute of Law, Research
and Reform
University of Alberta

BRAIBANT G.
Conseil d'Etat
France

BRAZEAU J.
Centre de Sondage
University of Montreal

BOOTH D.F.
I.P. Sharp Associates
Ottawa

BROWN C.
Leader of the Opposition Office
Ontario Government
Toronto

BRYSON G.
Alphatext Systems Limited
Ottawa

BURGER A.F.
Department of Finance
Ottawa

BURNHAM M. Elizabeth
The T. Eaton Company Limited
Toronto

BUTTERFIELD F.J.
Canadian National Telecommunications
Toronto

CARON Y.
Montreal

CARROLL J.M.
Computer Science Department
University of Western Ontario

CARSS T.O.
Bell Canada
Montreal

CHARLES W.H.
Law School
Dalhousie University

CHEETHAM A.
Ontario Credit Union League Ltd.
Toronto

CLENNETT M.C.
The Royal Bank of Canada
Montreal

CLERMONT M.
Banque Canadienne Nationale
Montréal

COOKE Susan
Credit Granters Association of Canada
Toronto

COOTE G.F.
Computer Data Processing Ltd.
Calgary

COSTA J.P.
Délégation à l'informatique
Conseil d'Etat, France

COTLER I.
Department of Justice
Ottawa

CROWSON J.S.
Department of Communications
Ottawa

DARLING P.A.
Computing Centre
University of Victoria

DESJARDINS Alice
Privy Council Office
Ottawa

DEUTSCH Dr. J.J.
Principal and Vice-Chancellor
Queen's University

DOLAN F.J.
Data Centre
University of Calgary

DORION Judge G.
Régie des services publics
Québec

ENDE A.H.
Federal Communications Commission
U.S.A.

FIELD F.W.
Bell Canada
Montreal

FIERHELLER G.A.
Systems Dimensions Limited
Ottawa

FORGET G.
Centre de documentation
Laval University

FOX R.G.
Centre of Criminology
University of Toronto

FREEDMAN H.A.
Dominion Bureau of Statistics
Ottawa

FUNK J.A.
Saskatchewan Telecommunications
Regina

GARDNER Capt. M.T.
Canadian Forces Headquarters
Ottawa

GALLOUEDEC-GENUYS F.
Centre national de la
recherche scientifique
Paris

GIRARD J.R.
Department of Eduction
Quebec

GLINSKI G.S.
Electrical Engineering Department
University of Ottawa

GORDON H.P.
Lawyer
Montreal

GRAHAM Prof. J.W.
Computing Centre
University of Waterloo

GOODFELLOW B.B.
IBM Canada Limited
Toronto

GOTLIEB A.E.
Deputy Minister of Communications
Ottawa

GOTLIEB Prof. C.C.
Institute of Computer Science
University of Toronto

GUTHRIE A.D.
Lawyer
Montreal

GWYN R.
Department of Communications
Ottawa

HANSEN B.
Committee of Presidents of
the Universities of Ontario
Toronto

HOLMLUND B.A.
Department of Computational Science
University of Saskatchewan

HARVEY L.
Control Data Canada Limited
Montreal

HAYES R.D.
Department of Justice
Ottawa

HEAP F.K.
Department of Supply & Services
Ottawa

HEENAN T.F.
B.C. Telephone Company
Vancouver

HILTON D.A.
Department of Communications
Ottawa

HOFLEY B.C.
Department of the Solicitor
General
Ottawa

HOULE G.
Bell Canada
Montreal

HUGHES C.J.
Department of Mathematics
University of Ottawa

HOWARD F.E.
Department of Communications
Ottawa

IRONSIDE Diana J.
The Ontario Institute for
Studies in Education
Toronto

IEVERS Miss Florence
Department of Communications
Ottawa

IRWIN J.W.
Retail Council of Canada
Toronto

JONES R.H.
Royal Canadian Mounted Police
Ottawa

JENKINS W.
Computer Centre
Queen's University

KATZ L.
Physics Department
University of Saskatchewan

KAUFMAN Dr. H.
Science Council of Canada
Ottawa

KEECH Dr. G.L.
Data-Processing Computing Centre
McMaster University

KENNEDY G.H.
Retail Credit Company of Canada Ltd.
Toronto

KIERANS Honorable E.
Minister of Communications
Ottawa

KING E.E.R.
Department of Communications
Ottawa

KINGSBURY L.D.
Imperial Oil Limited
Toronto

KOLTAI S.K.
Department of Treasury & Economics
Toronto

KUTT M.
Consolidated Computer Services Ltd.
Toronto

LAWFORD Prof. H.
Faculty of Law
Queen's University

LEAL H.Allan
Ontario Law Reform Commission
Toronto

LEDERMAN Prof. W.R.
Faculty of Law
Queen's University

LEGARE J.
Department de démographie
University of Montreal

LEGRIS Y.
Department of Communications
Ottawa

LIEBEL P.
Department of Communications
Ottawa

LINDEN R.F.
Department of Industry, Trade and Commerce
Ottawa

LATTA K.
Faculty of Law
Queen's University

MACDONALD Dr. J.B.
Committee of Presidents of Universities of Ontario
Toronto

MACNUTT J.
Department of Development
P.E.I.

MANNING E.G.
Computer Science Department
University of Waterloo

MARSH A.
Ecole de bibliothécaires
University of Ottawa

MASSICOTTE J.
Department of Communications
Ottawa

MCCLUNG M.
Secretary of State Department
Ottawa

MCGEE C.E.
Department of Communications
Ottawa

MCINNES G.A.
Alphatext Systems Limited
Ottawa

MCPHAIL Prof. T.L.
Department of Communication Arts
Loyola College of Montreal

MEZEI Prof. L.
Department of Computer Science
University of Toronto

MILNE J.D.
The Canada Life Assurance Company
Toronto

MURRAY G.G.
IBM Canada Limited
Toronto

O'CONNELL B.P.
Research Department
McMaster University

OGILVIE J.C.
Department of Psychology
University of Toronto

OLSON E.R.
Department of Justice
Ottawa

O'REILLY B.
Department of Communications
Ottawa

PATENAUDE P.
Faculté de Droit
Université de Sherbrooke

PATTERSON Z.R.
Ontario Department of Education
Toronto

PEARSON M.T.
Associated Credit Bureaus of Canada
Toronto

PHARAND D.
Faculté de Droit
University of Ottawa

POLLARD W.L.
London Life Insurance Company
London

POUNDER D.W.
Systems Dimensions Limited
Ottawa

RAYCRAFT G.J.
Ontario Credit Union League Limite
Toronto

REIMAN R.I.
Treasury Board
Government of Ontario
Toronto

RIBLER Dr. R.
Computer Sciences Canada Limited
Toronto

RICHARDSON L.E.
T-Scan Limited
Toronto

ROBB J.A.
Lawyer
Montreal

ROBICHAUD Dr. P.H.
Centre de Calcul
Laval University

ROBINSON Dr. P.
Department of Agriculture
Ottawa

ROBSON Dr. R.A.H.
Department of Sociology &
Anthropology
University of British Columbia

RODGERS I.
Financial Post
Toronto

RUSSELL J.M.
Systems Dimensions Limited
Ottawa

RYAN E.F.
Ontario Law Reform Commission
Toronto

RYAN J.W.
Department of Justice
Ottawa

SCHMEISER Prof. D.A.
College of Law
University of Saskatchewan

SCHNAITH R.A.
Univac
St. Paul, Minnesota

SCOTT D.B.
Department of Computing Science
University of Alberta

SEAMAN A.E.
Department of Communications
Ottawa

SEDGWICK G.G.
Lawyer
Toronto

SHARP I.P.
I.P. Sharp Associates
Toronto

SHARP Prof. J.M.
Faculty of Law
University of Manitoba

SHEPPARD C.A.
Avocat
Montreal

SKELLY Dr. S.
Department of Attorney General
Winnipeg

SMITH T.B.
Department of Justice
Ottawa

SOBERMAN DEAN D.A.
Law Faculty
Queen's University

SPEIGHT J.A.
Computech Consulting
Vancouver

SPICER E.J.
Library of Parliament
Ottawa

STEWART Gail
Economic Council of Canada
Ottawa

ST-PIERRE Prof. J.
Centre de Calcul
University of Montreal

TANNOCK B.W.
Shell Canada Limited
Toronto

TAPSELL J.E.
IBM Canada Limited
Toronto

TATEISHI A.T.
Department of Supply & Services
Ottawa

TAYLOR G.F.
Bell Canada
Montreal

TELLIER P.M.
Bureau du Conseil Privé
Ottawa

THOMAS U.
OECD Secretariat
France

THOMSON G.M.
Royal Canadian Mounted Police
Ottawa

THOMPSON G.B.
Northern Electric Company
Ottawa

TRUDEL J.P.
Commission des écoles catholiques
de Montréal

TURNER Honorable John
Minister of Justice
Ottawa

VANDER NOOT Dr. T.J.
Dominion Bureau of Statistics
Ottawa

WARE Dr. W.H.
The Rand Corporation
U.S.A.

WARREN R.G.
Department of Communications
Ottawa

WILLIAMS I.
Department of Sociology
University of Western Ontario

WILLIAMSON D.
Alberta Government Telephones
Edmonton

WILSON Helen
Department of Communications
Ottawa

YEOMANS D.R.
Department of Supply & Services
Ottawa

ZEAMAN Z.
CRESIGU
Montreal