CONFERENCE ON COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION, QUEEN'S UNIVERSITY, 1970.

Conference on Computers: Privacy and Freedom of Information.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

Notes for a speech

on

Policy considerations concerning the development of Teleprocessing and Data Banks

by

The Hon. Eric Kierans

Minister of Communications

Kingston, May 22, 1970

Release: 7 p.m. 22-5-70

On several recent occasions, I have publicly expressed concern about Canada's need to develop sound and imaginative policies so that we, as a nation and as individuals, can truly benefit from the advances that are being made in communications technology. Within the broad scope of communications technology, much of my concern, and it is reflected in the activities of the Department, has been centered on the sector of computer/communications.

Beyond any doubt, the marriage of computers and communications, of data-processing and telecommunications, represents one of the most significant technological advances of our time. It has given rise to the phrase "computer utility". Another desc ription, coined by John Diebold, is that of "data utility". No matter the name -- and there are clearly possibilities of misunderstanding in the use of a word such as utility -- no matter the name, it is the product that matters; and that product is the distribution to an ever-widening number of users, whether institutions or individuals, of ever-growing quantities of organized, structured, processed information and the distribution is performed at high speed, and over great distances.

I have said that this marriage between the computer and the communications networks represents one of the most significant technological advances of our time. Equally, and as a direct consequence of that technological fact, it

.../2

represents a potential social, political, cultural and economic advance of equal significance. Electronic libraries; national data banks; individualized instruction; electronic banking; the identification, by means of computer models, of national problems long before they develop. That list of potential marvels -- and it could easily be lengthened ten or one-hundred fold -- is already familiar, almost over-familiar. Some items on the list, because of technical and even more because of financial, limitations, will never happen. Other developments, which today we can barely imagine, will happen with unforeseen ease and speed.

For all those benefits we will also pay a price. Technology is not passive; it is a dynamic force working within and upon society. And its effects can be negative and destructive of our social fabric. One speaker to this conference has cited the example of pollution: very late in the day, almost too late, we have learned that the price we have paid for many job-creating, wealth-producing industries is the degradation of our water and air. We have learned, in other words, that technological progress is not always in fact progress.

.../3

To take another example, familiar to this audience -- that of CAI, or computer assisted instruction. The danger is not that CAI may not work, in a technical sense, or that it will be, as one authority as put it, nothing more than "an expensive, text-book page turner"; the danger instead is that computerized education will divorce student from teacher, that instead of being a complement to personal instruction it will become a substitute for it, and that, for all the talk of individualized instruction, the end product will be lock-step education scantified by the awesome efficiency of technology.

This conference is a step, and no more than a step, in exploring the potential -- and I emphasize the word 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 wholescale technological pollution to match our industrial pollution - a technological pollution which could end up with us re-ordering our social behaviour and priorities to suit the mechanical convenience of machines.

.../4

I intend to say no more on the issue of computers and the invasion of privacy. In the first place I am in no sense an expert. In the second place it is the business of this conference. However, I would like to express my great pleasure at the large numbers who are attending this conference -- computer manufacturers, designers, operators, users, representatives from the communications industry, lawyers, sociologists, and just plain interested individuals. I would like also to express my great pleasure that the Department of Justice, the Information Processing Society and Queen's University have joined with the Department of Communications to co-sponsor this conference as part of the Telecommission. The need for cooperation between government, industries and universities has become virtually an after-dinner speaker's cliche. This conference, is an example of that concept in productive action.

Having deliberately steered away from the subject-matter that is occupying you for these three and a half days, I would like instead to use the occasion of having before me an audience so widely representative of the computer industry, to raise a number of other questions within the broad field of computer communications.

A good place to start is the policy considerations surrounding the possible creation of a national computer-communications network, or networks.

The first characteristic about such a network that needs to be known is how large is it -- one that just covers the centers of population and of commerce, or the entire country. If this network is restricted just to the principal cities, then it will increase the regional economic disparity which is one of the principal causes of the strains upon the Canadian confederation. But if, in order to reduce that disparity, the network is extended beyond its natural economic boundaries, then who is to pay for the difference, and by what standards, and in what amounts.

A second issue is control of the network. In dealing with computer-communications we are dealing with one of the most dynamic industries in our society, and which, as I have said earlier, has enormous social, political and cultural as well as economic potential. At present Canadian ownership of the computer industry, and I have in mind here the entire industry from hardware manufacturing to the retailing of software programs, amounts to between 10 and 15 per cent.

.../6

Plainly only the most unremitting optimist could expect that Canada can ever become a major manufacturer of large computer mainframes.

In the field of peripheral and terminal equipment, where imaginative innovation can yield dividends, the prospects are brighter -- as the President of the Information Processing Society would be quick to explain, and proudly so.

But the real action and the real potential lies in the field of software -- in the development of programs, of information systems, of specialized services and languages, of data banks. I make no pretence of my concern, on the contrary I emphasize it, that in recent months a number of independent Canadian computer utilities or service bureaus, call them what you will, have encountered difficulties and have in some instances been sold to non-Canadian buyers.

Some of these difficulties have been caused by local and temporary conditions. These are the normal hazards of competitive enterprise. What does concern me is the long-term trend. A strong and viable Canadian presence in the computer industry is essential if we are to retain our ability to shape our future as we see fit and not as others may, unconsciously and unintentionally, decide. In seeking to ensure such a Canadian presence a whole range of options present themselves to Government, from reliance on the open market forces

to regulation, and in-between such alternatives or combinations as incentives, assistance, encouragement of effective rationalization, direct entry and so on. It is with these questions that we are grappling in the Telecommission, and the fruits of those labours will be published in order to provide an opportunity for comment, criticism, amendment, addition, improvement.

In this endeavour two difficulties arise. The first is the subject itself. Computers are a very recent topic of public debate, and the technology and patterns of business are in a state of almost continual change. The target therefore moves, and changes, even as one studies it. Secondly, Government and the computer industry have talked very little to each other in the past -- and except on the basis of individual contacts, never before on the broad scale now under way. The Telecommission is providing one opportunity for an exchange of views. This conference, in its particular field, provides another link in the chain. But a great deal more dialogue is needed -- a system for exchanging information about information systems.

Coming back to possible policy questions I have mentioned as possible options available to Government those of incentives and assistance. Regardless of the financial ownership of companies in the computer industry, it is evident that if Canada is to exploit the enormous possibilities opened up by the computer revolution then we must develop in this

.../8

country a pool of computer talent and expertise. Specifically we are going to have to consider assistance for research, manpower training and for pilot projects -- projects which are either directly in the public interest or which can subsequently be developed by Canadian industry.

Other questions which we are going to have to consider have their basis in law. The location of computer centers in integrated systems and the control of both the equipment and the information contained in those systems affects the definition of our national sovereignty. As I have already said publicly, if vital Canadian data banks are located outside our borders, then any rules we may develop concerning privacy and freedom of access will be inapplicable in those instances -- and our sovereignty will have been diminished.

A further legal issue involves patents and copyright. Apart from the legal dimensions there are other aspects of the general problem that require international consultation and consideration. International co-operation in the domain of telecommunications has a successful century-old history. The extent of this co-operation has steadily expanded as new systems have been introduced. The advent of computer/communications systems will raise issues such as the development of equipment and international technical and operating standards, either within the existing institutions of the ITU or less specialized bodies like the OECD.

.../9

Before Canada can effectively engage in any such international initiatives our own domestic policies must be clearly defined. And this brings me back to my starting point and the planning, coordination and development of national computer-communication networks. For such an undertaking, the data processing and telecommunications industries, must work closely with government and with major users, both actual and potential. For cooperation to be effective, careful attention should be paid to the institutional character of any co-ordinating body, its composition and its terms of reference. While ultimate responsibility for policy rests with the government, a larger body of opinion and expertise would be essential in examining such questions as the selection of computer services for meeting specific problems, the commercial practices of the computer/communications industry, including charging and costing formulae used in the trade; the inter-connection of computer and communication services and particularly the equipment and technical criteria so that large scale information systems can be effectively utilized. The sole function of such a body or central agency would be to stimulate the computer/communications industry. To be effective, it would however have to be concious that it was co-ordinating planning for a powerful industry and that the purpose of this planning was to serve not only the objectives of the industry, but also the social and economic goals of the nation. One instance of of such a national goal would be to promote the extension of services on an east-west rather than north-south axis.

.../10

One other area where a central planning group could play a useful role would be in the development of the criteria to be applied to the development of computerized information systems - or if you will, data banks.

The development of computerized data banks is still in its infancy. One of the oldest civilian systems, the U.S. MEDLA RS medical information service, is only six years old. Most computerized data banks are still being planned -- such as the National Research Council's Science and Technical Information System -- or are as yet only being dreamt about. This gives us time, but very little time, to consider such basic questions as: what types of banks should be developed in the national interest and in what order of priorities; what types of information should be collected, by whom; who will have access to the banks; who will control input to the banks; what should be the architecture of data banks.

We should not pass over lightly the institutional characteristics that large data bank systems are taking on and some suggested frameworks for proposed systems. In practical terms the form of the body vested with control of a data bank determines its legal personality and this has a great bearing on a number of issues, including liability for negligent actions, the right of access to the information and in economic terms

its financial viability. Theoretically one could construct a model based on the proposition that all information in data systems should have no constraints on its accessability. But in practice such a model would be unworkable. Similarly, there are unanswered questions with respect to systems to which special interest groups may wish to restrict access. For instance, should a social scientist willing to pay a subscription fee be allowed access to a medical record system. Or for that matter should a journalist have access to a legal data system which had been constructed and was operating on behalf of the legal profession?

Within the DOC we are aware of several proposed computerized data bank systems that are at various stages of development. Some of these are highly innovative, others are merely a compilation of existing manuall y controlled files. Some have specific applications and are aimed at a particular category of user, others are more universal. Some systems have easily visualized commercial applications and as such their creation depends to a large degree on the ability of their promoters to market the idea. Other proposed systems are non-commercial in a market sense but possess a corresponding social value and their promoters have turned to the government to find the necessary funds to devise and develop these systems.

.../12

One of the Telecommission studies is concerned with data banks and is examining a variety of systems covering such classifications as law, medicine, consumer information, scientific and technical information. Each proposal is different, but each has in common the enormous cost needed to move it from concept to reality. Often the bulk of these costs relate not to the computer technology, but to the organization of the information, so that it can be fed into memory. A question that is immediately raised is who should bear the expense for the creation of these banks, and to what extent, and in what form. For instance if a legal data bank or a medical data bank is to be used primarily for the benefit of the legal or medical profession, is there a valid reason why the financing of the bank should be undertaken by the federal government. And if the answer is yes, then on what basis should selection be made if public resources are limited (and I assure you they are limited). Should a legal data bank be created before a medical data bank, but after a scientific and technical information system? Should the government be expected to back more than one system in a particular field? Should the universities, who are playing a valuable role in the research and development of computerized information systems be encouraged to continue this work when the commercial application of particular projects looks fuzzy or remote? And not the least important, should the government

.../13

sit back and let data banks develop without direction, risking on the one hand that systems with commercial applications will be located and operated from the United States? And on the other that systems of great potential benefit to Canada will never be developed at all.

There is one other large policy consideration that I should like to mention. The group that is gathered here represents both the problem and the answer. In the field of computer communications where we are encountering new problems, some as complex as our society has ever faced, an effort must be made to ensure that the right combination of human skills is brought to bear on the issues. Because the technology is moving forward at such a rate there is a need not only to add to our reservoir of human skills but to update and re-educate those people who have experience in the computer field. And in settling the large issues of how this technology is going to be developed, and for what ends, it is necessary that we maintain a flexibility so that people of different disciplines and of differing backgrounds can be heard and can give of their experience and wisdom. The trained multi-disciplinary manpower needed to move into a computer/communications age is also a public policy question.

If we have learned anything in the past few years, it is that our technology cannot solve all our problems and that it indeed creates new ones. The systemization of information should not be thought of as the systemization of human understanding. As our world becomes more complex it becomes more inter-dependent. It was the communications industry that perfected the operational methods now commonly described as systems engineering. Unfortunately there does not yet exist a comparable methodology which might be called "systems policy". And two essential ingredients of any such policy-making system would be common sense and sensitivity. If we as a society prove ourselves incapable of either recognizing or understanding these interdependencies between technique and ultimate purpose, we stand the risk of becoming the prisoners of our own short-sightedness and the slaves of our own technology.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

OPENING SESSION: Privacy and Openness as Social and Legal Concepts

The Right to Privacy in a Computronic Age

by

The Hon. John N. Turner

Minister of Justice & Attorney General of Canada

THE RIGHT TO PRIVACY IN A COMPUTRONIC AGE.

It is perhaps of no small significance - and indeed of some historic value - that this is the first Conference ever held in Canada on the problems of Computers: Privacy and Freedom of Information. But 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, though the philosophic import of the problem was no less serious here in Canada. Accordingly, while vigorous public debate and legislative exercise had been proceeding for some seventy years in the United States, there was during this same time no public discussions here in Canada, no legal writing of any kind, no legislative debate, no jurisprudential inquiries. The first article on the right to privacy was written in 1961, and the first real legislative exercises of any note did not begin until the mid-60's.

And so it is, then, that the jurisprudential underpinnings for this opening panel discussion on Privacy and Openness as Social and Legal Concepts originate south of the border. For it is here that the philosophic thrust and legal imperatives in respect of the right to privacy were born. And although the philosophic contours must be appreciated within the Canadian context, and while the legal imperatives must be Canadian formulations, the

philosophic and legal experience grounded in some eighty years of serious intellectual and legal inquiry ought not to be ignored.

In 1890 a young lawyer co-authored an article in the Harvard Law Review on the "right to privacy" that was to become a classic of its time. The authors defined privacy as, "the right of each individual to determine to what extent his thoughts, sentiments and emotions shall be communicated to others". But the profundity of the article resided as much in prophecy as in principle. For in a brief - and sometimes ignored - reference, it warned of the "mechanical devices which threatened to make good the prediction 'that what is whispered in the closet shall be proclaimed from the housetops'". Some 40 years later the young lawyer, now Associate Chief Justice Brandeis of the U.S. Supreme Court, outlined the dissent that was later to become the law of the land in language that became the philosophic measure of the right to privacy for all lands:

> "The makers of the Constitution undertook to secure conditions favourable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfaction of life are to be found in material things. They sought to protect people in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the Government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men."

But if privacy is the most comprehensive of rights, the most comprehensive of techniques - and here in Canada - can be used to destroy it.

-- A remote controlled amplifier and microphone no larger than the head of a pin can capture a conversation and transmit it by wire for 25 miles.

-- A parabolic microphone without wires or radio transmitter can catch the conversation of people in a boat in mid-lake and record it on shore.

-- The switching of a single wire can convert any telephone in Canada into a live microphone conducting sound even when the telephone is in its cradle.

-- Cameras the size of a cigarette can photograph a room two blocks away by moonlight, or photograph actions in a dark room when equipped with infrared film.

-- Infrared light techniques permit a room to be watched and photographed from an adjoining room through apparently opaque walls, while wall microphones, of course, can hear and record anything said in such a room.

-- Radio pills substituted for the subject's aspirins and lodged in his stomach can transform him into a living electronic beacon.

-- The investigator's dream - making his subject a walking transmitter and enabling the investigator to hear everything the subject says to anybody else, or even what he mutters to himself - can be realized by the wiring of a person's clothing.

-- And an example of the installation possibilities of existing microminiature transmitters is provided by a transmitter so small that it has been mounted as a tooth in a dental bridge.

These illustrations are but some of the miniaturization possibilities in a technetronic environment. Indeed, to some of you they may not only be well known but shop-worn as well. For the technetronic arsenal here described ignores the application of computers to communications - or the advent of what I would call the "computronic age". Yet an increasing proportion of the transmissions carried by our communications networks involves data in digital form as against the conventional oral or voice transmissions. While the law lags then, technology races, and once again the scientists have beaten the lawyers.

The corollary to all this, as revealed in testimony before the Commons Committee on Justice and Legal Affairs, and of particular importance to those of us who have been given the temporary custody of the administration of justice, is that your telephone can be tapped, your office bugged, your files photographed, your physical movements monitored, your communications recorded - all this without your having any right or recourse or any protection in law. Indeed, the Orwellian society of 1984 appears sanguine alongside the miniaturization of our technetronic or computronic society. The open society has become the bugged society. The struggle for freedom is being mortgaged to the parabolic microphone. The zones of privacy are being occupied. There are no more sanctuaries.

But 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. Indeed, if any further testimony of the essence of the right to privacy as coterminous with life itself is required, it can be found in a recent article on privacy in the Yale Law Journal. Prof. Charles Fried describes this existential need in moving terms as follows:

> "Privacy is not just one possible means among others to insure some other value, but it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence. To make clear the necessity of privacy as a context for respect, love, friendship and trust is to bring out also why a threat to privacy seems to threaten our very integrity as persons. To respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion."

But privacy has implications not only for the individual but for the collectivity as well. For, what must be realized is that the right to privacy not only goes to the core of our being as individuals, but to the core of our being as a society or state. John Stuart Mill said that, "The worth of a state in the long run is the worth of the individuals composing it." A state that demeans its individuals demeans itself; a society that mocks the privacy of individuals mocks itself. To pose, then, the question of surveillance and the right to privacy in terms of the needs of the state versus the rights of individuals is

to pose the question not only in asymmetrical terms but in confusing ones as well. For the right to privacy is organized around the principles of both the rights of individuals and the needs of the state.

> "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas. When dissent from the popular view is discouraged, intellectual controversy is smothered, the process for testing new concepts and ideas is hindered and desirable change is slowed. External restraints, of which electronic surveillance is but one possibility, are thus repugnant to citizens of such a society and to the society itself."

(President's Commission on Law Enforcement and Administration of Justice summarizing the relationship between privacy and the democratic order itself.)

But to some, the threat to privacy from electronic eavesdropping, in both an individual and societal sense, pales before the privacy-shrinking enormities inherent in the computronics of data surveillance. It is here that the new information transfer technologies, with their capacity to accumulate, manipulate, store, retrieve, transmit and disclose information, come into their own. For, as a number of authorities, including Professor Arthur Miller of the University of Michigan Law School, have pointed out:

> "The computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances and our associations will be bared to a wide range of observers."

Indeed, Professor Alan Westin himself has warned that: "Unless the issue of privacy is in the forefront of planning and administration of future computer systems, the possibility of data surveillance over the individual in 1984 could be chilling". Professor Westin may be uncharacteristically optimistic here. The possibilities of data surveillance are already beginning to have a chilling effect. (I was delighted to read that Dr. Westin has been appointed to direct a nation-wide study on computer data banks and the right to privacy for the Computer Science and Engineering Board of the National Academy of Sciences in the United States.)

The development of a national policy in respect of information systems and the right to privacy (as Dr. Kelly Gotlieb of the University of Toronto in his Conference paper points out, the term "information system" is more inclusive than that of "data banks" and perhaps more appropriate for our purposes) requires first of all that we get some data about the information systems themselves. In other words, 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.

It is only after a descriptive inventory of where we are in information systems technology has been achieved that we can undertake the prescriptive task of formulating the kinds of administrative, legislative, technological and organizational measures to preserve the integrity of privacy in our data-generating society.

Such prescriptive formulations ought to concern themselves with the legal imperatives which will govern the legal rights and obligations of all the participants effecting, and affected by, information system technologies. Such legal imperatives will be grounded in the policy options which may be posed as follows:

-- What agencies, both of a public and private nature, shall be authorized, under what procedures and for what purposes, to collect what kinds of information, to be stored in what kinds of systems? Professor Sharp, in his Conference paper, has advanced certain legislative proposals in this regard in terms of a licencing and regulatory scheme in respect of our information systems.

-- Who will have access, under what conditions, to what kinds of information, for what purposes?

-- What kinds of procedures will be available, under what circumstances for validation and verification of what kinds of information?

-- What kinds of information will be transmitted to whom, under what procedures, and for what purposes, and what kinds of evidentiary rules will govern such transfer and disclosure?

-- What sanctions will be available to whom, under what circumstances, and with what procedures?

Information systems increasingly integrated with computer data banks have become a necessary and inevitable resource for decision-making in the public and private sectors. But many of these memory drums contain highly personal - and prized - information about the citizen, i.e., his health, education, family background, financial status, employment status, credit rating, civic associations, criminal records, etc. This information - some of which may be inaccurate or misleading - is being relied on heavily by both private and governmental agencies to decide whether individuals get jobs, credit, insurance, government benefits, or even whether they are the subject of regulation and prosecution.

But there is still another hidden and rather frightening variable here. Computers, as Herman Kahn and Norbert Wiener pointed out in their study, "In the Year 2,000":

> "...may be able to apply a great deal of inferential logic on their own - they may become a sort of transistorized Sherlock Holmes making hypotheses and investigating leads in a more or less autonomous or self-motivating manner, all the while improving their techniques as they accumulate information about any kind of behaviour that authorities decide ought to be observed. New legal doctrines will need to be developed to regulate these new possibilities for just looking."

Information, then, is power. Computerized information systems where the computers themselves become programmed for self-generation allow for an enormous amount of power to be wielded by very few people having access to, and controlling, the information systems.

It would make participatory democracy all but a sham; a new transistorized eliteism could manipulate our wants and needs.

The law itself will have to have a creative input if we are to assure any balance between the needs and inevitability of information systems on the one hand, and the rights and needs of privacy and dignity on the other, as well as the integrity of the democratic polity itself. By 1980, 80% of all Canadians will be housed on less than 1% of our land mass. Our cities will resemble "urban hives". The new cybernetics of an increasingly urbanized computronic environment will surround us. Science and technology will result in new forms of electronic surveillance, psychological surveillance, and data surveillance. Indeed, scientists are already experimenting with the applications of computer technology to brain-wave analysis to join the more conventional forms of psychological surveillance involved in personality testing and polygraphing; while national data banks, commercial reporting agencies, computerized transactions and the like are already making us the greatest data-generating, privacy-invading society ever known. Indeed, data-generating societies may well remember what we have chosen to forget. The orbit of privacy will be an ever-shrinking one, but the need for privacy will be more paramount than ever. The law must ensure that the right to privacy remains sacrosanct.

ADDENDUM:

Freedom of Information

Mr. Chairman, there is another side to the right to 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 a 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. What is necessary, then, is a Freedom of Information Act entitling the individual to information which the government authority has arbitrarily seen fit to withhold. Indeed, as Professor Hugh Lawford of Queen's University 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 government information to be exempt from disclosure. This included, inter alia, matters such as defence or foreign policy secrets authorized to be kept secret by executive order, etc.

. . 12

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.

5(6)

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 1

Privacy and Openness as Social and Legal Concepts: - The Right to Connect and Disconnect

by

A. E. Gotlieb

Deputy Minister of Communications

CONFERENCE

SUR

L'ORDINATEUR, LA VIE PRIVEE ET LA LIBERTE D'INFORMATION

UNIVERSITE QUEEN'S

21-24 MAI

1970

PRIVACY AND OPENNESS AS SOCIAL AND LEGAL CONCEPTS: - THE RIGHT TO CONNECT AND DISCONNECT

Communications technology has made giant strides in the last few years. Satellites, microwave systems, lasers, coaxial cables and computers are being put to work in ways that give them an increasingly broad influence on our lives. These achievements of technology are producing a contraction of time and space that very vew human beings have fully grasped or exploited in our generation. Not only have communications between urban centres and isolated regions of countries become much easier, but it is now possible to establish instantaneous communication over vast oceans and continents much more efficiently than ever before.

No member of an audience such as this can be in any doubt that the proliferation of communications networks combined with computer technology has triggered an information explosion. The impact is revolutionary, both in terms of the volume of information communicated and of the numbers of people inter-connected with each other. Man is becoming connected to the entire world. The local and universal dimensions of man's interests and existence are tending steadily to move closer together, as he stands inter-connected with what is near and remote, as he connects with change at home and upheaval abroad, with the fate of manking everywhere, with the sweep of ideas and of history itself. In effect, the nervous system of man is merging into the new nervous system of the world, the vast and expanding networks of computers, commu-

nications and information systems. And by extending himself, by communicating at a distance - - tele-communicating in fact - - man is changing his historic, traditional nature: instead of the natural man, the institutional man, the God-seeking man of our philosophies, our technology is creating the communicating man, and man in search of, in need of information on a scale and at a speed that nothing in historical experience has prepared us for.

In Canada, the Department of Communications has been assigned the task of ensuring that national communications systems are developed and deployed for the greatest possible good of all Canadians. The complexity of modern technology and the expanding needs of contemporary society require that governments formulate policies to ensure an equitable distribution of technology's benefits. Unless technology can be harnessed to human needs there will be an understandable revolt against technology, or worse still, a harnessing of human values to serve the dynamics of the machine world. We must begin at once to plan -- and to plan far in advance, if technology is not to decide our future for us.

We now know all too well that the impact of technology reverberates in various unforeseen ways, through the decades or generations that follow its introduction. When we think of nuclear energy, the automobile, pesticides, and other significant technical developments of our time, we begin to suspect that the

waves of their reverberations may carry us right out of existence. In the field of communications we understand little but we fear that the medium itself may come to have a sort of transmuting effect on us and the generations that (hopefully) will follow. These were some of the considerations that prompted the Department of Communications to establish last year the very wide ranging Telecommission to study virtually all aspects of communications in Canada, to identify the key social, economic and technical problems, and to gather together, as quickly as possible, all the information essential to the formulation of conclusions by the Governments.

In its analysis and treatment of the problems of communications, our Department sees, in an embryonic form, the development of a new notion or concept, or more exactly, of new human right: 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.

This is why I believe we must identify, as a basic goal of Canadian communications policy, the need to ensure that the greatest number of Canadians, whether in our cities or in the remotest parts of our country, have the widest possible access to the greatest amount of information, at the lowest possible

cost. Information flow and population movement may not be entirely unrelated. Migration from the country to the city might very well be accelerated even beyond today's projections, if, in future, far greater discrepancies were to develop now, significant as they are, between the amount of information available to city-dwellers and that available to people outside the growing urban clusters of North America. In an age where all useful knowledge will be stored and retrieved automatically, the ability to access such information remotely through telecommunications might possibly help to increase the chances of maintaining, for longer periods than now, in the various distant parts of Canada, the minimum of population basic to the development of our resources. At the political level, the electronic networking of information might help to develop and maintain the viability of that eastwest axis of Canada which is essential to our very existence.

While I am firmly convinced of the importance of identifying and securing to every Canadian the right to communicate, I think we must recognize the equal importance of securing to every individual another right, an obverse right, --the freedom of every Canadian to disconnect or, in other words, the right not to communicate. One of the fundamental principles of our society 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 the information offered to him. But this 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.

It is usually said, and I suppose correctly, that the information explosion which is now getting underway offers dazzling prospects for all who are interested in human progress. Mankind will be able to become more educated, more cultured and more catholic in his pastimes. I accept -- I don't think there is any choice -- that there will be a time - not so very distant - when we shall have remote and automatic access to a vast continental system of stored information. No longer will we be obliged to sift through stacks of documents to find references or records that we require in our work. We will consult the omniscient computer.

This ubiquitous information system will, we are told, again correctly, not be limited to a few select fields. It will be massive, all-embracing, and will involve virtually every area of human activity. As I have said, all useful knowledge will probably be stored this way, and a lot of useless knowledge as well. Little that touches humans will remain beyond its reach, and certainly not the privacy of the individual. Information will be available not only on a person's level of education and career performance, but also on everything related to his credit rating, his debts, the way he spends his money, his physical and mental health, the operations he has undergone, his criminal record, if he has one, and a host of other matters. In this electronically informed society, the computer can, in short, keep abreast of

everything significant that relates to the individual and with a great deal that is insignificant. Those with access to this information can thus obtain a tremendous capacity to observe and assess an individual's behaviour in relation to any number of situations where his past conduct or individual qualities might be considered of some relevance.

Several developments are transforming the traditional methods of obtaining and dealing with information to produce this result.

Before the advent of the computer, for example, 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 portrait of a person that might emerge from such files was necessarily fragmented since each one contained information on only one aspect of his life, (his credit rating, say, or his brushes with the law) and exchanges of information between different files were rare. The computer, however, makes it possible and economic to store, combine and transfer masses of data in such a way as to give access to complete information on any given person. Secondly, the tie-in with communications systems can make the information available to anyone, virtually anywhere. Thirdly, while electronic eavesdropping have been available for a long time, they are now so sophisticated that descriptions of their capabilities read like science fiction or a James Bond novel. With these devices the computerized

portrait of an individual can be filled out without the consent or knowledge of that person. These new surveillance techniques can be used also to monitor the transmission of information from computerized data banks. And finally, governments, insurance companies and other large agencies and concerns are gathering more and more information about more and more people. The various needs of government, including requirements for information for social security and revenue purposes, the dictates of marketing and the need for information on human behaviour arising from a variety of sources in the criminal field, all are producing a tidal wave of information about individuals touching virtually all aspects of their interests and activities. Any combination of these pools of information in personal data banks is likely to have very far reaching implications for those whose lives are compiled in bits and connected into the computer-communications systems of the future.

A very fundamental question, then, is whether society should allow any type of information concerning an individual to be collected. A related question is should society allow such files to be combined and stored? Yet another basic question is: whether the information, once collected, should be accessible to just anyone? All these questions can be reduced to one fundamental issue: is there such a thing, in our society, as the right to privacy, and if so, has it acquired the status of a basic human right?

I think it is difficult to deny that in our own social framework, there does exist a private "domain" that is recognized to belong to the individual, and that he will either refuse to communicate whatever lies within its bounds, or will do so only with reluctance and to a carefully selected audience. What dimensions of one's life lie within such a domain? What is the acceptable scope of the individual's "private" life? There is no simple answer to this question but we know, or can sense, that just as there is a territorial imperative which requires that for his psychological well-being each individual must command a space which he can call his own, so there is what one might call a solitary, or private, imperative as crucial for our stability and fullness as human beings.

In the private domain, there may be found the desire to be 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.

One of the difficulties of defining privacy arises from the fact that it is, of course, not of equal importance in all societies.

Some privacy requirements that exist in our own society - an individual's desire for a home in which to live with his family, for example - are lacking in societies where housing is something for a larger family that includes parents, grandparents and sometimes even uncles and aunts. The way a society is governed also has a bearing on notions of privacy: individual secrecy may be much less important in a communist state than in a capitalist one. Even within a single society, the changes it undergoes may cause the notion of privacy to evolve as time goes by. Finally, not every individual agrees with his neighbour as to what constitutes his privacy, or his neighbours' privacy.

The need, in our own society, for each individual to have some measure of privacy is, I think, basic to his equilibrium and to his peace of mind. The time an individual is able to spend alone or in the company of close associates allows him to get to know himself better, to appraise himself, and thus to decide where he stands in his life, what are his failures, his goals, his ambitions and what he needs to develop his full potential. It also enables him to set aside for a few moments the role he has to play in normal life, and rediscover himself. This in turn enables him to do things that he might not do if he knew they would become public knowledge. Privacy may thus help us from being or becoming everyman, it might help us to resist the seemingly irresistable drive to conformity in an age where the computer treats all data as the same.

It is at this point that an over-informed society, a society that knows and wishes to know everything about an individual, can become a danger. Four kinds of invasion of privacy can be noted:

1. interference with solitude or with private affairs;
2. the divulging of embarrassing personal information;
3. publicity that puts an accused person in a poor light in bringing him to public attention; and
4. using another person's name, or resemblance to another person, for one's own purposes.

In this future society where the computer is the repository of all knowledge, information will probably come to be manipulated by fewer and fewer highly skilled people. This increases the danger that the gap between the administrators or super-administrators and the rest of society may widen, no matter how deeply felt are the professions of faith in democracy. The saying that knowledge is power is probably true today; it will be far more true tomorrow. Except that the saying should be changed to information is power, with information, and therefore power, increasingly flowing to those who know how to manipulate our electronic systems of communication. The individual may come to feel to an ever increasing extent, that he is spied-on in an information - dominated society, and his behaviour may be influenced, as I have suggested, to the point where he prefers to act in the same way as those around him, and not set himself apart. The result would be an

atrophied society whose members would show no initiative or willingness to innovate.

With electronic memories, it will be possible,

to collect all possible data on a given individual, and this body of information will follow him throughout his life like a ball and chain. In the past, the dispersion of information on a particular person did afford him some guarantee of oblivion. There was a possibility that as a result of the difficulty of assembling a complete record on someone and making all information accessible, some features of his past life might remain buried forever in files. Memory banks will change all this, and the slightest error a person commits, once recorded by the computer, will never be forgotten. A pitiless society may grant no citizen a second chance. Ins't the right to be wrong an essential element of human liberty? At this point someone might say: while a personal file may contain information about a misdemeanour, or mistake, committed by the individual, that information would never be divulged, or misused - that it is not the computer which decides its use but society. This defence misses the point: <u>All</u> information, good or bad, important or trivial, that is recorded, is noticed - and anything that is noticed will, eventually, be used. And so the basic question returns - why create a system of record-keeping which automatically records and stores more information about ourselves than we would like anyone to know. Is the gain in efficiency worth the loss, potential or real, of humanity?

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? What can or should be the role of governments? First and foremost in importance, we must not forget that the law cannot solve everthing. For example, it is powerless, I think, to prevent one of the most worrying aspects of an information - rich society - the expanding gap between those who manipulate information and those about whom information is being manipulated.

Privacy, as such, is not protected by legislation anywhere in Canada outside British Columbia. At the international level, both the Declaration of Human Rights and the Covenant on Civil and Political Rights contain provisions to protect the individual against illegal or unwarranted interference in his private affairs; neither document, however, imposes a legal obligation on states.

It is clear that the notion of privacy has a number of different aspects, and is bound to evolve as society evolves. 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. A recent report by a committee of the House of Commons deals with this matter and suggests that the Criminal Code be used to outlaw electronic eavesdropping. It recommends that the use or disclosure of information obtained by such methods should also be forbidden unless it is essential to the investigation of criminal activities, in which case the authorization of a judge will have to be sought by a minister of the Crown.

Writers interested in the right of privacy have made a number of suggestions about how protection of privacy can be achieved. There has been an enormous amount of literature on the subject and suggestions multiply as to what to protect and how to do it. There have been proposals that every person have the right to know whether files are assembled on him and if so what specific information the dossier contains. Proposals are made for protection against the police in relation to their information gathering techniques, protection against the government in relation to security files or the formation of generalized files, protection against credit companies in relation to the data they keep and purvey. There are proposals that extend to protection of industrial information, protection against false information, protection against unprofessional ways of obtaining data, protection against the misuse of this information, protection against misrepresentation, possibly and a whole host of types of intrusion.

In Manitoba, an inquiry into credit bureaux in Canada proposed licensing of such offices and compulsory disclosure of information to any person on whom they report, with the subject being provided with a right to examine the report if he or she so desires. In Ontario, private members' bills have been introduced that seek to regulate the dissemination of personal data stored in computers. Under these last proposals, anyone affected would be able to check the accuracy of information concerning himself, and demand the deletion of anything incorrect, unfair or out of date.

It has been said that protection of privacy is possible only at the cost of the greater efficiency that an automated information-society will bring us. I believe that men want both access to the greatest possible amount of information, and respect for their individual privacy. This is a challenge, but it will not be an impossible one, provided we begin to meet it at once and with a deep sense of commitment and of conviction that early and positive action must be taken.

In undertaking this task, I think it essential that we do not think of a right of privacy as a single simple right which requires protection. The best and only effective way of attacking the problem of protecting privacy is to approach it as one of expanding and defining the civil liberties or rights of man that need to be protected in a rapidly changing technological society, and in particular, in a society in which information on the indivi-

dual is becoming far more easily obtained, maintained and communicated. And in that search for a human and effective definition of privacy, the need of society for information will have to be balanced against the need, and right, of individuals not to have information about themselves misused, and not to have certain types of information used at all.

Even if, as I said before, the law connot solve all the problems that science and technology will create for the individual, it will be called upon to play a fundamental and significant role in his protection in an age of virtually total electronic information systems. 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; we can, in fact be confident that man and his liberties would be very seriously threatened. I am convinced that a variety of types of legislation will have to be adopted in the near future. I am convinced that, in order to deal successfully with the dangers inherent in a computer society, privacy will have to be protected in a much more effective way than it is now by existing law. The gap between technological development and legal regulation connot 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 communications promise to bring about.

What will be required in a computerized information society, in fact what we need now, is the same concentration of legal talent that, in the past, has gone into the protection of property, its definition and promulgation as a legal system. We must apply these same talents to the definition of human rights and the construction of laws that are needed to protect the privacy of the individual in its various aspects. We cannot afford to wait. We must act now.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 2

The Computer and Privacy: No Relationship!

by

Dr. T. J. Vander Noot

Dominion Bureau of Statistics

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

RESUMÉ OF

The Computer and Privacy: No Relationship!

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

The most important point in this paper is that the content and use or misuse of information in a data base is far more important than the methodology of data storage and retrieval. Information systems and information misuse existed prior to the advent of the computer and to blame the computer for current difficulties is merely to avoid looking at the real problems squarely.

Only in one area, residual disclosure, is the computer a meaningful element in the problem configuration. The ability of the computer to provide even statistical data by smaller and finer breakdown does increase the potential risk of divulging information about an individual accidentally. However, the needs of a modern, complex society for more and better social data must also be met.

The Computer and Privacy: No Relationship!

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

Recently, the Toronto Globe and Mail reported a speech by Earl Warren, the retired Chief Justice of the U.S. Supreme Court, under the headline "Warren says wiretapping, data banks 'harm rights of individual irreparably'". The actual sentence in Chief Justice Warren's speech, upon which the headline writer exercised so much poetic license, was "The universal use of such information harms the standing of individuals irreparably."1/ The dilemma of our society is rather neatly portrayed by this single minor incident. The distinction between the misuse of information and the use of data banks apparently is too subtle to make a good headline. Thus, in the interest of emotional rather than rational news reporting, data-banks are being equated with wiretapping and other electronic invasions of privacy.

While this Globe and Mail article may characterize the problem, definitions and a brief survey of the field are necessary before going further. Most data processors today tend to equate the terms "data bank" and "information system", and define them as "a methodology for storing, maintaining and

retrieving data on user demand".2/ (Note that this definition does not mention the computer.)

Following this definition, the number of information systems in use today must be very large. Almost every computer installation has at least one system that will fit the above definition. Since most corporate information systems deal generally with the internal operations of that corporation, most of these can be excluded as being of no real concern to the general public. It is only when data, held by a corporation, concerns individuals or other corporations that the public rightly may be concerned. In this category we would have to include the data files of government agencies such as National Revenue or the Dominion Bureau of Statistics, the criminal files of the RCMP, business organizations such as Dunn & Bradstreet or Standard & Poor's, and finally the material held by credit bureaus and banks. What is, perhaps, most important to the general public in its evident concern about information systems, is the recent discovery that "it is much less expensive and more efficient to share information than to reproduce it"3/. The public feels that data too freely shared is tantamount to general publication.

Consideration of computerized information systems, however, has no relevance in any discussion of civil liberties or privacy. This statement, which will surprise many, and shock some, can be illustrated in a number of different ways. The most

common computerized information systems in use in business today are the inventory control systems. Usually an inventory system consists of a data-base with records for each separate type of item in the inventory. Information can be added to or retrieved from this base on demand. To an information scientist or a data processor an inventory control system is identical to the system used by a credit bureau or a police record system, since the general methodology of all such systems is identical. If the systems cannot be differentiated on the basis of methodology, any concern for civil liberties must be in terms of the type of data to be stored and the potential use of that data. Furthermore, information systems have existed for a long time without the computer being involved. For instance, a telephone book fits virtually any meaningful definition of an information system.

A data processor cannot solve a problem that has not yet been stated. The issue of confidentiality should have been raised in regard to information systems, either electronic or manual, far sooner. In general, custodians of information have avoided dealing with the very difficult question of what is confidentiality. This was accomplished either by examining each case or request for data individually or by making the information available only to members of some "in-group". "Individual examination" may have been adequate prior to the "information explosion" but it is certainly not adequate today. And credit bureaus, with their "private club" approach, have demonstrated an inability either to maintain accuracy of files or

to use restraint in passing out information. The custodians and users of the data must agree on what constitutes the right of data access as balanced against the right of privacy.

As the electronic hardware has been increased in size and speed the possibility of holding more and more data, retrievable in more and more subtle ways has increased. If the data processor has any involvement at all in the crucial question of privacy, it has been in his effect as a trigger for the concern of the general public. But invasions of privacy are the result of misuses of the data retrieved and not a function of the storage medium. If a personal diary is stolen and used for blackmail, is the bookbinder who manufactured the diary guilty? Is there any recourse open to an individual if his name is misspelled or the wrong number is shown in the telephone book?

Not all data processors would agree to this limited definition of the role of the data processor in the privacy issue. Some, like Hoffman,4/ have approached the problem of privacy in a rather mechanistic manner. The belief that the problems of safeguarding are "mechanical" stimulates them to incorporate more and more complex techniques for limiting and safeguarding access to a data base. Shielding on terminal lines, pass-words, keys, plastic code cards, and armed guards, are the tools of the mechanistic approach. Petersen and Turn have listed the mechanistic threats to privacy as follows:

Accidental
  User error
  System error
Deliberate, passive
  Electromagnetic pick-up
  Wiretapping
Deliberate, active
  Browsing
  Masquerading as another user
  "Between lines" entry while user is inactive but on channel
  "Piggy back" entry by interception and transmitting an "error" message to the user
  Core dumping to get residual information5/

Perhaps the mechanistic approach is appropriate in one sense. The function of the data processor may be to prevent unauthorized access to the base by data processing means. The sole duty of the data processor, therefore, would be to concern himself only with the physical security and proper operation of the system.

But, proper operation of systems is not the evidenced concern of the public. The public seems to be more concerned with the data itself. The data processor perhaps rightly, or perhaps wrongly, has not concerned himself with purposes to which his system is put, nor with the type of data included. A recent editorial in one of the trade papers gives some indication that this attitude is changing, and is quoted here in its entirety:

Is Privacy Necessary?

Some people are beginning to argue that privacy is not only no longer possible but unnecessary. They say that if everyone knows everything about everyone else, then all information becomes valueless.

The argument might have some merit if people were entirely rational. But they are not. All people are emotional to some extent.

Test yourself. A man applies for a job. He has all the experience required and makes a very favorable impression during the interview.

Then the dossier arrives from Personnel Data Bank Inc. It notes the man's father was convicted of murder (but does not mention he was later found to have been the wrong man), that his mother was on welfare (but does not mention that this was made necessary by the wrongful conviction of her husband and the fact that she had five children to support), and so on.

Would you hire this man? If you say yes, there is a serious question whether you are reacting to a theoretical situation differently than you would to an actual one.

Give it some thought before saying that privacy isn't necessary.6/

It seems to me that accuracy and data use are the crucial questions. All of the "horror stories" being told about computerized information systems seem to revolve around mistakes or lack of completeness in stored data. And this is where the solutions must lie, in the demand that constructed data bases be accurate, complete, and responsible. I am not an authority on law and I do not know the problems involved, so the solution seems simple to me. Broaden the slander and libel laws. Make every holder and/or publisher of data liable for damages and/or fines payable to the wronged individual. I wonder how many errors there would be in the telephone book if the telephone company had to give a year's free service for each error?

Professor Alan F. Westin, Professor of Public Law and Government at Columbia University, carried this thought one crucial step further by saying there is a need for "a' writ of habeas data, commanding government and private organizations to produce the data that they have collected and are using to make judgements about an individual, and to justify their using this."7/

Economically rational businesses must equate costs with benefits. Statistically speaking, credit bureaus and the telephone companies are very accurate in maintaining their files. But they are willing to accept some degree of inaccuracy simply because it is very expensive to make them more accurate than they are now. If mistakes were to be made very very costly in terms

of penalties paid to the wronged party, then greater accuracy would become economically rational.

There is a very different and difficult problem in governmental statistics. As social scientists have become more sophisticated, and data retrieval less expensive, there has been a drastic increase in published data and the demand for even more data. Inadvertant disclosure of data about an individual becomes increasingly possible. Here is a problem that cannot be ignored.

The Canadian Statistics Act represents a type of "social contract" between the Dominion Bureau of Statistics and the data-providing public. It enables D.B.S. to collect data from individuals to satisfy the legitimate information requirements of the country and provides protection to individuals by prohibiting the publication or dissemination of individually identifiable data. Hence the Act guarantees that no harm will come to an individual as a result of his compliance with the Act. (Even the publication of aggregate data may result in generalized "harm" to specific individuals, for example changes in legislation.)

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 of D.B.S.; 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 firm or other respondent.

Information collected and published by D.B.S. is designed to be of use only for statistical purposes. Such analysis does not require information about identifiable respondents, and it, therefore, follows that the D.B.S. will not provide information pertaining to a particular individual or other respondent, nor does it publish or otherwise make available the records it collects in a way that permits the identification of these records as being specific to particular respondents. The second provision simply provides for the safety of data against fraud, and establishes the accountability of D.B.S. personnel.

Confidentiality seems to be a legal concept, and is the legislator's way of saying: "Don't publish or make available information collected which may be harmful to the individual respondents who provided them." The public has a more diffuse concept of harmfulness in that he is clearly concerned with his privacy and privacy seems to involve keeping information secret. Thus, there is a real distinction between confidentiality, the legal concept, and privacy, the public concern.

Here may be the crux of the problem. Is the public really concerned about keeping all knowledge about himself "private", (that is secret) or is the real concern over having "private" information used "against" the individual. Simply and baldly stated, the society needs certain information from the individual and corporate members of that society so that economic and social planning can have some basis in fact. Since the benefits of good planning are so great, the Statistics Act says that the respondent can tell the truth (even to admitting certain improprieties) without fear of reprisal.

In spite of having massive files based on reports from individuals, the general practice of publishing only aggregates tends to protect D.B.S. from most serious "invasion of privacy" problems. There is one type of disclosure, however, that is specific to a statistical organization like D.B.S.--residual disclosure. This occurs when two or more sets of data taken <u>together</u> could allow the identification of information 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. Usually this province is grouped together with another province whose corresponding total, by itself, is publishable. If in another table the "publishable" province is identified separately,

the corresponding total for the first province can be obtained by subtraction--a residual disclosure. In Canada, this is a particularly vexing problem since data for the Census of Manufactures is collected jointly with provincial agencies (with the full knowledge and consent of respondents). It is difficult, however, to convince a larger province, which is entitled to publish its results, to forego publication to safeguard the confidentiality of respondents in a smaller province.

The public also needs to be protected against the burdens of providing the mass of information required by the modern state. Information for statistical purposes is only one part of the burden. Statisticians have a clear responsibility to reduce the burden if the needed data can be extracted from data provided by the public for administrative purposes. This is an increasingly rich source of statistical information since the administrative activities of modern governments encompass ever wider spheres.

All concerned would benefit if statistical agencies could get access to administrative data, 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. In this context, the provision of the Statistics Act that identifies the purpose of data collection (whether directly from the individual or indirectly from an administrative agency), as being

for statistical purposes has a bearing. Statisticians must strive to clarify the fundamental distinction between information to be used for statistical, or for other, purposes.

In summary, safeguarding confidentiality in the governmental area can lead to duplication of effort by the statistical agency and the administrative agencies, or in fact even between statistical agencies. Leaving the collection to administrative agencies can be a useful, in fact, sometimes unavoidable method of avoiding duplication and can result in high-quality statistics under the right circumstances. It is not, however, a solution which is necessarily the best method for avoiding duplication. Joint collection, with the primary duty of collection vested in the statistical agency, may be a better solution. In the latter case, care must be exercised that the authority of the Statistics Act to collect data is not used as an umbrella for the provision of individual returns to administrative agencies, unless this is done with the explicit permission of respondents. A statistical agency should have unimpeded access to administrative data for statistical data (but this should not become an excuse for abandoning data collection to administrative agencies). At the same time the statistical agency must strive to maintain in the public mind the fundamental distinction between data for statistical and administrative purposes. It should also have a genuine concern for safeguarding the confidentiality of individual returns.

From the point of view of a professional data processor, confidentiality is the problem of the data collector. From his point of view, retrieval from census files is no different from selecting a book in a library. The data processor needs to know the answer to such questions as which data items are to be secure, should the confidentiality rules apply to retrieved tabulations rather than to individual data elements, and what is the procedure, in precise terms, to determine the confidentiality of a particular tabulation. And so we are back to the definitional problem.

Thus in a broad sense there exist two separate problems. The users of statistical data are not interested in specific individuals and, therefore, the concern of the statistical agency is to prevent inadvertant identification of an individual respondent. The users of credit bureau type services are, on the other hand, frequently concerned with data about a specific person. The problems are different but often confused.

Professor Westin, feels that "primarily the focus of system administrators has been on the devising of hardware and software measures (to protect privacy)... these are expenditures of time and money in the right cause and they deserve to be encouraged... but... the basic questions that need to be faced here are political not technical. They are matters of social policy to be worked out by balancing the values in civil

liberties against those of efficiency and secrecy in government operations."8/

While I think that Westin has summarized, in large part, the essence of this paper, I feel that I must close on a more personal note. The opinions expressed in this paper are primarily my own and do not represent any official view. That statement, true of the preceding, is even more true of the following.

As a professional in the field of data processing, I am sick of being cast as the villain in the tragedy of the invasion of privacy. Ask the personnel man why he wants to know at what age an employee stopped wetting the bed. Ask the credit bureau manager why he can remember to record the filing but not the dismissal of a suit against someone. Ask the political demagogue why he sounds the alarum against computers, but not against his own file of peccadillos that other people have committed.

Concern for the misuses of information should have been expressed long before this by those concerned with civil liberties. This I say as a professional data processor to all "fearless" defenders of civil liberties: you have hidden behind the Luddite fears of the public long enough. The computer is not to blame. Your own delinquency and timidity in attacking those who misuse data are to blame.

FOOTNOTES

(1) Wills, Terrance, Globe and Mail, 29 January 1970.

(2) Glossary of Data Processing and Statistical Terms Dominion Bureau of Statistics, 1969.

(3) Ramey, J.W., "Computer information sharing--threat to individual freedom", Proc. of Amer. Documentation Institute, 1967, pp. 273-277.

(4) Hoffman, Lance J., "Computers and Privacy: A Survey", Computing Surveys, Vol. 1, No. 2, June 1969 pp. 85-103.

(5) Petersen, H.E., and Turn, R., "System Implications of Information Privacy", Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp.291-300.

(6) Editorial, Computerworld, February 4, 1970, Page 8.

(7) Quoted in The National Observer, 26 January 1970, Page 12.

(8) Quoted in Datamation, February 1970, Page 161.

NB: Portions of this paper appear in a different form in a working paper being prepared for the Conference of Commonwealth Statisticians by Dr. I.P. Fellegi and this author.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 3

Computer Data Banks and Security Controls

by

Dr. Willis H. Ware

The Rand Corporation

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

COMPUTER DATA BANKS AND SECURITY CONTROLS

W. H. Ware

Resumé

There is not today an established "data bank industry", nor are the technical risks of operating computer-based data banks widely understood. Moreover, the financial incentive of the data bank operator favors the user of the bank rather than the private individual. For these reasons, it is argued that strong government intervention and control is necessary to protect the privacy and reputation of individuals. The state-of-art for information safeguards in computer systems does not permit a handbook approach to the subject; only general principles and guidelines can be stated. Suggestions are made for controls that can protect information within the computer and govern its divulgence to authorized users. Ideas are proposed for the role of the government agency in the matter, its interface with and control over operators of data banks, and inferentially, the need for relevant legislation. The individual's position is defined, and his expectations identified. Views are expressed on the responsibility and liability of data bank operators and data sources relative to such things as identification of legitimate users of the bank, divulgence of information, and accuracy and completeness of information.

COMPUTER DATA BANKS AND SECURITY CONTROLS

W. H. Ware*

The RAND Corporation, Santa Monica, California

TORONTO CONFERENCE - MAY 1970

The issue is to safeguard the privacy and reputation of the individual by guaranteeing that information about him in computer files is not revealed indiscriminately. This implies that information contained in computer files must be protected and released only to authorized users. In discussing this matter, my point of view will be that we must accept data banks as desirable and as serving a useful purpose for society. Certainly, existing computer data banks on criminal activities contribute to better law enforcement; existing credit reference data banks assist society by making it more difficult to pass bad checks which, in turn, means a financial saving to society. Thus, I will not discuss the fundamental question of whether data banks are desirable or not; but I will consider what can be done to protect and control dissemination of information in them. This discussion cannot be a how-to-do-it handbook; the general state-of-the-art is not yet to that point. Rather, this paper is a collection of ideas for consideration and debate.

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

Perhaps the largest and best organized systems for protecting information are those devised by governments to safeguard national defense information and national secrets. Since such systems have been in existence for a long time, it will be instructive to consider them both for insight and as a framework for thinking about the problem. They are usually established through legislation and/or executive order, and typically include the following features:

1) Classes of information are defined whose divulgence is considered a threat to the interests of the country. The threat is defined for each class.
2) Procedures are defined for establishing that individuals are trustworthy to receive information.
3) The principle is established that an individual receives information only if it is necessary for performance of his job.
4) Procedures are created both for controlling dissemination and for protecting information, no matter in what form it may be recorded; e.g., documents, magnetic tapes, etc.
5) Penalties are defined for deliberately revealing information to unauthorized recipients.

Data banks may not need as full a treatment as accorded national defense data. However, we should consider the implications for data banks of those features that have been found desirable to protect national secrets.

Consider what is probably the most hazardous circumstance: a data bank that receives information from specified sources; that is maintained in a computer at a central location; and that serves users who are remotely connected to the computer by communication lines. The several parts of the problem are as follows:

1) Information that is inserted into the data bank must either be known to be correct, or have some level of confidence attached to it.
2) Information, once within the data bank, must be revealed only to individuals authorized to receive it.
3) Identity of individuals requesting information from the data bank must be established before the information can be released.

First, it must be understood that the problem is a system one, which must be attacked from a system engineering point of view in the broadest sense. If handled in a bits-and-pieces fashion, the finest of safeguards in one part of the system can easily be circumvented by loopholes elsewhere.

Consider item 2 first. The protection of information within a computer system has already received attention in the context of national defense information, and a few such systems are operating with appropriate security safeguards. There is, therefore, an initial set of ideas that have been formulated and to which technical attention has been given.

To outline what is necessary, consider a data bank of information that is within a computer system; is considered to be valid; and is to be dispensed to users on request. There are five points that need attention:

1) Obviously, physical protection must be afforded the computing central and demountable storage media. All the safeguards in the world will be to no avail if magnetic tapes or magnetic disks can be stolen or copied by unauthorized persons.

2) Ideally, the communications should be protected by some form of encryption or physical protection of the circuits. Practically, this may not be essential because the amount of data on any one communication line will probably be small. On the other hand, wiretaps are very easy, and penetrating the system through its communication circuits is a serious threat that the system designer must consider.

3) A multi-user system (especially one which is accessed through a remote console) is, in effect, a timesharing system that itself must have appropriate computer hardware safeguards. There may be needed--depending on the precise details of the application--bounds registers to segment the memory, an interrupt system to control activities within the computer system, memory protect features,

and two internal modes of machine operations, one of which is privileged to the monitor program.

4) Software safeguards must also be provided. There must be a mechanism to control user access to the files. There must be audit trails to keep track of what users are doing and what data each has asked for. There must be mechanisms for alerting operations personnel to unusual situations, especially marginal conditions in the hardware or malfunctions of the software. There must be mechanisms for the system to self-test itself to guarantee continuity of the hardware and software safeguards.

5) The system's administrative and management controls must be security conscious, and include such things as:

   - o Provisions for monitoring and controlling the action of system operators;
   - o Procedures for loading certified copies of the software and verifying that it did correctly load;
   - o Procedures for controlling movement of and physical access to demountable files.

These five points have received considerable technical attention because each is relevant to currently operating systems that contain defense classified information; also,

each in some measure is an aspect of resource-sharing systems in general.

Notice in passing that certifying that the software is correct, completely designed, and contains no unanticipated paths through it is a major technical problem. It is one thing to establish that software will do what it is supposed to do. It is quite a different and more difficult thing to prove that it does not do what it is not supposed to do, especially when hardware malfunctions or unusual user actions occur. Once it is certified to be correct, the software must be guarded against unauthorized changes.

Now let us discuss points 1 and 3, which are larger issues of concern to this conference. These are intimately connected with directly protecting the privacy and reputation of an individual.

Given the initial assumption that data banks serve useful purposes for the public, are cost effective, and will be in existence, it follows that each individual wants to make certain that: 1) information in the bank about himself is correct; 2) information is divulged only to those who will use it in his interest or to his benefit; and, 3) he has recourse for damages in the event the users or operators of the data bank willfully or negligently mishandle the information.

Even though technical safeguards can help enforce these principles, I feel that ultimately they will have to be

passed in law. Therefore, government intervention is necessary. It follows that enforcement and monitoring of the law will be necessary, and I would, at least in the near term, center that responsibility in a governmental regulatory body. This may seem a strong position, but I will support it later. Furthermore, I would rather begin too strongly and weaken controls as experience shows it possible, than recover from awkward oversights after the fact.

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:

1) 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.
2) 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.
3) A complete description of the safeguards in the system (physical, hardware, software, communication, personnel, and administrative/management) that protect information and control its divulgence.
4) 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.

5) A complete description of the audit processes incorporated in the system, and the audit information that will be made available for periodic review.

6) 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.

7) 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.

It is obvious from my position that I feel that a government agency not only must carefully investigate proposals for data bank business, but that it must also audit such business from time to time to assure continuity of safe and legal operation. The job of the regulatory agency is partly highly technical, and relevant expertise must be available. It is clear that the closeness and depth of inspections and investigations must depend on the nature of the data bank. For one which contains information that cannot seriously harm an individual, governmental intervention can be minimal; but for one which contains very extensive dossiers on individuals, the control must be

correspondingly greater. Since governments themselves are talking of establishing data banks, what I have implied for private operators should apply to government agencies.

Next, let us turn our attention to the users that the system serves. First, what determines who they are. Most data banks will sell services; thus, the nature of the bank and the aggressiveness of its marketing will tend to identify the user group. The operator must accept prime responsibility for certifying that his users are as they represent themselves. It would seem desirable to require a business man to present the usual credentials of his business status (e.g., business licenses, offices, staff, equipment, etc.) before being accepted as a customer of the system. The provisions of communications' secrecy acts would seem to be applicable since users will receive information as a privileged communique and should therefore be liable for willful or negligent transfer to other parties. If the user is another data bank, the operator of the first data bank must take additional safeguards. 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, be they other data banks, individuals, other businesses, or government sources. I believe that data sources cannot be anonymous and thus immune from legal action; they must accept responsibility for carelessness or negligence.

From the individual's point of view, there must be appropriate legislation enabling a person who has been maligned or damaged because of the activities of a data bank to take prompt legal action, and to seek redress against the users, operators, or data sources. There are special situations where the individual probably should have a legal, court-created document certifying that some action has been taken. For example, consider the person who has been arrested and accused of a felony; 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.

This may all seem overwhelming and too much, but I have tried to explore the worst-case situations. I have tried to suggest some kinds of information safeguards that could be implemented, and may have to be done. Certainly, there is no general recipe that will *a priori* describe the controls relevant to every data bank. Depending upon the data it deals with, the completeness of records on each individual, the users it serves, the threat from subversive

penetration, etc., specific protective mechanisms and procedures will have to be evolved.

There are some general observations that are relevant to my position that strong governmental controls are desirable. Presently, there is no "data bank industry" as there is an automobile industry or a motion picture industry. There are no trade organizations; and thus, self-policing is not likely. Furthermore, the financial incentives of the data bank operator favor the user. It is from the user that the operator derives his revenue, and the individual is hard put to cause the operator serious financial damage. Business is unavoidably profit oriented, so there is no substantial intrinsic motivation for the operator to surround his data bank with a complete set of information safeguards. Moreover, an operator may be technically ignorant of the risks in his system, or unaware of the ease with which it can be penetrated.

Finally, consider what can happen if data banks proliferate widely and without control. We see all around us situations that were recognized after the fact and are now out of control and harmful to society; the many kinds of pollution are a prominent example. Protection of the individual's privacy and reputation is already recognized as essential to society's health; I would rather not have data banks become the problem that pollution has. 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.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 3

THE INFORMATION UTILITY

by

D.F. Parkhill

Director General

Policy, Plans and Programs

Department of Communications

Ottawa

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

THE INFORMATION UTILITY

Even under the best of conditions, the art of prophecy is a difficult process and this is particularly true when the subject is a dynamic technology like computerized information systems. For technical change in the field of digital computers has been continuous and pervasive for over twenty years now and during that time has produced at least three complete generations of systems and set the stage for the emergence of the fourth. Consequently, when we attempt to look into the future and divine the direction which "needs and technology" appear to be taking us we run a serious risk that some quite unexpected technical development will completely discredit the assumptions upon which our predictions were based.

Within the limits set by this qualification, however, it does seem safe to state that, for the rest of this decade at least, 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.

The term "information utility" as used here denotes a combined computer/communications system which makes available a wide range of different information processing services and capabilities to a multitude of diverse, geographically distributed users. These utilities take many different forms and collectively are involved in a myriad of different applications including all of those tasks for which conventional computers are normally employed, in addition to a host of others that only become feasible through the multi-user features. Regardless of the form however, these new systems differ fundamentally from the normal computer service bureau or data bank in that the services are supplied directly to the user in his home, office or factory without requiring the physical transport of data between the customers and the central facilities. In fact, it is convenient to regard them as comprising a new class of resource sharing systems in which a rather nebulous commodity called "computer", or more correctly "information power" is shared in a convenient and economical manner

among many remote customers.

This "information power" is a much more complex commodity than, for example, electric power or telephone service. In it are contained elements of mathematics, of information retrieval, of communications in all of its myriad forms, of publishing, of human and machine actions and interactions, and even of mind. Its definition involves complex combinations of time; computation rates; instruction repertoires; data and procedure bases; peripheral equipment characteristic and usages; communications speeds, capacities and access times, and so on. Figure 1 is an attempt to portray something of this complexity.

APPLICATIONS

The general technical advances that have made possible the Information Utility can be briefly summarized as follows:

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.

... 3

6. The technique of time sharing has made direct dialogue between man and computer economically practical.
7. Techniques of man-computer interaction have been developed that permit true intellectual partnerships between men and machines so that the special capabilities of each are blended together in a harmonious whole. These techniques have been successfully applied to many fields including engineering design, information retrieval, medical diagnosis, problem solving and computer programming.

As a result of these advances, the growth of remote access time sharing systems is now proceeding at a phenomenal pace with new systems and new commercial services being announced every week. In fact, the chorus of doubters who were so vociferous in their downgrading of time sharing two or three years ago now seems to be silenced and many observers are predicting that, by 1975, something between 75 and 90 per cent of all computers will be operating in a shared remote access mode. The questions that are now being asked consequently no longer concern the merits of time sharing per se, but rather the relative difficulties and advantages of applying it to particular applications.

Any complete list of possible applications would resemble the index to the Encyclopedia Britannica. Consequently, an attempt to separately analyze each possible application would result in a document of encyclopedia dimensions. On the other hand, a great deal can be learned by lumping the different applications together under suitable headings in a logical classification scheme. One such scheme that has been found useful employs six basic categories:

... 4

REFERENCE SERVICES

The first commercial applications of the on-line real time and time shared modes of operation were those which involved access to a common data base by many remotely located users. Early applications included airline and railway reservation services, order tallying, and stock market quotation services. Today, the range of application is being further extended and specialized information networks are evolving for handling such diverse forms of information as policy records, credit reports, medical files and scientific data of all kinds.

The evolution of such specialized networks is bound to continue as more and more of the myriad social and occupational groups of the moderm community come to appreciate the advantages of direct access. Some of the broad categories of services that might be provided include:

Professional - legal, medical, law enforcement, scientific, engineering, pharmacy, agriculture, etc.

Business - credit, real estate, marketing reports, regulations, prices, trade data, etc.

Consumer - consumer testing and satisfaction reports, product specifications and prices, product availability, advertising, etc.

General Information - political and economic data, historical, travel, weather, entertainment, etc.

These are further summarized in Figure 2.

It is obvious that these categories could be expanded indefinitely until they included the totality of human knowledge and, indeed, it is towards exactly this end that the evolution of the information utility is directed. In the words of Robert Fano, the Director of Project MAC, it will become

"the depository of the data base and information processing procedures of the community". This depository will, in the long run, draw upon and integrate the resources of all of the specialized utilities so that it becomes a gigantic electronic encyclopedia, continuously distilling the essence from our society and making it available at any desired level of concentration to everyone.

FINANCIAL SERVICES

No aspect of direct access computer utilities has received more attention than their application to the world of finance. Some applications, those concerned with ready access to financial data are, of course, partially covered by the reference services category but there are many others and, just as in the reference services case, they are leading to specialized networks. These include:

Investment Nets concerned with security transactions, market analysis services and stock quotation service.

Insurance Nets capable not only of providing routine services to insurance companies but even of generating tailor-made policies on-line for individual customers.

Banking and Credit Services. Both the banks and credit agencies have been particularly active in opening up the "Direct Access Age" and are currently heavily involved in such activities as the development of professional billing services; the provision of on-line teller terminals, sometimes integrated with management information services; and the establishment of banking and credit networks.

As a result of these and similar developments, it is likely that, in the near future, we will see the credit card idea merged with the concepts of

... 6

computerized banking and credit bureaus to create a new type of universal financial utility whose customers will identify themselves by means of a universal credit card or "money key". As time goes on, it is likely that this "money key" will replace both the check and most normal currency as a medium of exchange. In fact, in both America and Europe, key experiments aimed at exploring the possibilities of such automatic transactions are currently underway. These experiments could eventually lead to an integrated worldwide financial network that will permit a customer to make money key transactions anywhere in the world. The range of services offered could also grow to eventually encompass every type of financial transaction, no matter how complex or trivial it might be.

When this happens, the Financial Utility, illustrated in Figure 3 will have available within its files a complete, immediately accessible electronic record of the current and past financial status of every customer from billion dollar corporation to school child. Bank balances, obligations, credit ratings, earnings (current, projected and past) data on all of these and more will be contained in the records. As a result, the flow of money between individuals, organizations, or even nations, will involve nothing more than an automatic transfer of information within the memory banks of the utility. In effect, all of the world's myriad financial institutions will have been integrated and transformed into a single vast electronic information system.

GENERAL BUSINESS SERVICES

Both the financial and reference services applications are, of course, deeply involved with business in all of its aspects. Nevertheless, there are many other areas of business life that could profitably use the services of a direct access computer utility. Some of these have been lumped together under the broad heading of General Business Services and are shown in Figure 4.

GENERAL COMPUTATION SERVICES

Calculation, in one form or another is, of course, interwoven with just about all of the applications that are discussed in this paper. Likewise, many of the functions included under the heading of General Computation Services in Figure 5 have already appeared elsewhere, either as functions within a larger application category, or as in the cases of reference data and planning, as major categories. Despite this, it was felt that the three major application categories shown: vis., Design, Business Computation and Automated Laboratory Services were sufficiently different from the applications that have been discussed hitherto to justify separate treatment.

EDUCATIONAL SERVICES (see Figure 6)

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. Progress along these tracks will be continuous at a pace that will be separately controlled 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.

PRIVATE DATA STORAGE AND RETRIEVAL

Implicit in most of the discussions in this paper has been an assumption that, in addition to providing computational and other services, the various systems would also make available private electronic storage files to which only the authorized user or his designee would have access. And, indeed, many existing public systems do provide such private storage facilities.

It is likely that, as the cost of providing such storage decreases and proven methods for assuring privacy are developed, computer files of this type will come to replace the majority of orthodox private data storage systems in the home as much as in business. One of the most significant features of this kind of file will be its dynamic nature. Thus, since the actual storage mechanism will be tied closely to powerful data-processing facilities, much of the onerous task of file organization will be delegated to these facilities. Complex data manipulation, editing, formatting, indexing and search routines will be available to the users and will introduce new dimensions to the usefulness of data storage systems.

RELATION OF APPLICATIONS TO SYSTEM CHARACTERISTICS

Earlier in this paper, Figure 1 portrayed some of the many factors involved in a definition of "computer power". For any information utility, the relative importance of these factors and the ways in which they interact are, to a large extent, dependent upon the applications that the system is designed to support. For example, if the application of the system is to be restricted to the single job of storing and retrieving information, then there will be no requirement for either a customer programming capability or for the extensive computational capabilities at the central processor. Thus, both the organization of the central machines and their program structure can be optimized around the data manipulation and file searching problems. On the other hand, there may

well be a need for storage of voluminous amounts of narrative and pictorial information in a rapidly searchable form and for its transmission to and reproduction at the user's console.

Again, if the application is basically a routine business processing one, invoice production, credit checking or inventory control, for example, then the full facilities of a General Purpose Business oriented computer will be required at the central station but, once more, there may be no need for user programming. Instead, an extensive library of packaged prewritten programming systems will be needed, each designed to handle a particular application for a whole industry, and hopefully, capable of satisfying with only minor modification the needs of many different customers. Many of the Financial, Educational Support and General Business Services applications fall into this category.

At the other extreme are the systems where customer programming is a major element in meeting the users' needs. In fact, the interactive operating mode which only becomes economically feasible, except for the very smallest machines, with time sharing, is in itself a major asset for the programmer.

THE PROMISE

It should be apparent from the broad scope of the applications just described that the information utility is destined to have a major impact upon our society. In fact, the social importance is implicit in the term "information power" for information is, in a very fundamental sense, the basic stuff of human society -- the true élan vital, if you will, whose communication and application in a billion different forms makes us human. Consequently, quantum jumps in our ability to handle information are invariably marked by fundamental changes in the nature and quality of society.

The term "post industrial society" is now increasingly used to describe the new society towards which the most technologically advanced nations now seem to be evolving. This society has been described as follows by J. Servan Schreiber in his justly renowned work "The American Challenge" --

"Not only will it be a richer society, but a different kind of society since, beyond a certain level, wealth is measured not so much by a higher standard of living as a completely different way of life".

In this new society, the developments that are the subject of this report will play a central role. For, in the post industrial community, just about every activity whether in the arts, sciences, industry, education or government will center around and, in fact, function through the ubiquitous computer networks. The "completely different way of life" promised by Schreiber therefore could include:

(1) Growth of Service Retailers: It is likely that the universal abundance of "raw computer power" will lead to an explosive growth of three new areas of entrepreneurship known as "service retailing". Instead of owning of renting computers, service retailers would rent memory capacity and processing capability; i.e. "raw computer power" from an organization known as a "raw computer power purveyor", fill the rented memory space with their own and their customers' proprietary data and programs, and then retail their services to their remote customers through the links provided by the telecommunications carriers. One would expect to find a multitude of different organizations represented in this category. They could include private companies, foundations, governments, educational and charitable institutions and even individuals. Some would be small, while others would be large. Some, like banks and loan agencies, might be heavily regulated

... 11

by appropriate government agencies while others, such as those concerned with the same of computational service, would be as free from regulation as any other competitive business.

One area where this could bring about some interesting changes is the publishing business. An author, for example, might do his writing at the keyboard of his personal utility console. His product would take shape in his private files in the central computer and, to publish, he would simply notify the utility of the existence of his work and authorize its inclusion in the public files. Once in these files, it would be freely accessible to all the other utility customers via the viewing screens of their own terminals. Utility fees, royalty payments and the like would be handled automatically, with a direct transfer of credits to the author's royalty account every time someone accessed his document. Similar arrangements could apply to every other type of creative work -- newspapers, magazines, motion pictures, computer programs, data banks and so on.

(2) An Economy of Abundance, largely automated and integrated so that all of the myriad industrial, distribution and business functions will become in effect a single distributed machine. Although this economy will be capable of turning out goods and services of a quality and in numbers that seem fantastic today, it will require very little human labor and most people, in the words of Schreiber, will enjoy "far more leisure time than hours of work".

(3) Individualized Computer Assisted Instruction providing each student with the equivalent of a private tutor embodying the best judgment and total experience of the world's greatest educators. Education will also become a continuing process largely independent of age and geographical location; i.e., no one will ever be further from the classroom that his local "fireside computer terminal".

... 12

(4) Decentralization: With the development of a "communications affluent" society in which the techniques of television, computer graphics, computerized data bases, data-processing and normal telecommunications are combined and their services made universally available via "fireside" terminals, many of the pressures for urbanization may be reversed. If people can access and manipulate any piece of information without leaving their homes and simultaneously interact with other people and machines as easily as if they were sitting in the same room with them, then there would seem to be little reason for concentrating workers in large office buildings. Just as was mentioned for education, they might better conduct their routine business activities from the comfort of their homes and gather together only for formal affairs, laboratory work and social occasions.

Eventually, with the production and distribution processes largely automated and with shopping, entertainment and business transpiring largely via telecommunications, the need for people to live within easy commuting distance of their business, school or shopping facilities will also vanish. It should be possible for people to live in any part of the country and eventually the world and still partake fully of all of the social and economic amenities that we associate with urban life. A family, for example, might live on a mountain top in British Columbia even though the husband "works" in Toronto, the son goes to school in Halifax, the daugher in Montreal and the wife does her shopping in London, New Delhi and Paris.

(5) Universal Access to Knowledge: The reference services mentioned earlier eventually will provide universal access to the complete store of human knowledge. The contents of the Lenin Library, of the British Museum or the Library of Congress will be instantly accessible at every man's terminal whether he lives in Yellowknife or Toronto. Combined with the teaching utilities mentioned earlier,

this universal access to information is bound to profoundly modify our traditional educational concepts. What, for example, is the value of those forms of education that are based upon the memorization of factual material, when every man can know any fact merely by approaching his fireside terminal?

(6) Greater Freedom of Choice for Consumers: The widespread incorporation of computer control in the manufacturing process and of computers in the performance of financial transactions should eliminate much of the need for standardization of products; ie., insurance policies, automobiles, appliances, furniture, etc., that is currently necessary for efficient operation and give the consumer much greater freedom to tailor his purchases to meet his own unique needs.

(7) True Participatory Democracy: The national computer networks will provide a natural medium for increasing the direct participation of citizens in the political process. Beginning with electronic opinion sampling, extending next to electronic vote-taking in local elections and referenda, later to national elections, it could eventually permit everyone to vote directly on all major issues and in effect extend the town meeting concept to the entire nation.

This list, of course, could be continued indefinitely but it does seem obvious that even if only a few of the possibilities mentioned come to pass, they still vindicate Schreiber's prediction of a "completely different way of life". Within this way of life, there is a common thread that ties together all of the possibilities and constitutes the true promise of the computer utility. This is the promise not alone of change, for change can just as easily be bad as good, but rather of large scale improvements in the quality of life for everyone. Taken together, these improvements add up to an infinitely freer life than any to which human beings have ever before dared aspire -- literally a life of limitless horizons in which human intelligence will be free to develop to its ultimate limits.

For Canada, these possibilities present us with what may be our supreme challenge. For, by aggressively and imaginatively exploiting the promise of the information utility, Canada could leap frog decades of normal development and become the world's first post industrial society. Within this new Canada, the universal availability of information power could magnify by orders of magnitude the economic and intellectual capabilities of our people and lift the nation in a gigantic quantum jump to an unprecedented level of achievement.

THE DANGERS

Unfortunately, there is also a darker side to the information utility and it requires little imagination to see some of the dangers that might face us if certain of its capabilities were to be misdirected. The technical advances that have made possible the information utility 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 networks -- 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.

Hopefully, however, out of this Conference will come recommendations for remedial measures that will bring the problem under control. Consequently, until the nature of these recommendations is known, it would be presumptuous for me to draw any hard conclusions. A model set of safeguards however might well include features like the following:*

*Some of these were suggested by Prof. John McCarthy of Stanford University in his "Bill of Rights" for privacy protection -- The Scientific American, Sept. 1966, P. 72.

-- Licensing of all data banks in which individuals are identified by name.

-- Licensing and bonding of all employees of data banks.

-- Specification by a government body of the rules governing access to all data banks and the programs that enforce them.

-- 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.

-- Every person has 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.

-- There is a public record of every access to an individual's file together with the name of the person performing the access, the purpose and the authority.

-- It is 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.

-- Improperly authorized access to an individual's file is a serious crime punishable under the criminal code by severe penalties. In addition, the party whose privacy is breached has the right to sue for damages.

The opposite side of the privacy coin is the problem of freedom of access. This is not likely to be a major problem for the immediate future but could become extremely serious as general information utilities evolve. For, as technology advances, it is likely that such systems will gradually replace the more orthodox

edia -- newspapers, radio, television, etc., as methods of mass communication. t is obvious that such monolithic oracles could easily represent a major threat o the freedom of expression that is the lifeblood of a democratic society. onsequently, stringent measures will be required to ensure that all ideas are eely aired and to guarantee equality of access. A constitutional guarantee f absolute freedom of speech within the information utility under all circumstances one obvious measure. Unfortunately, however, it would not solve the limitations hat an individual's pocket book might place upon his ability to exercise his onstitutional rights. Consequently, it may well be that serious consideration ould be given to making the facilities of the system available free of charge everyone. In addition, just as in the privacy case, criminal penalties and ivil redress should be made available to deal with those who attempt to manipulate he public files for private advantage or improperly restrict an individual's ght of access to those files.

FIGURE 1

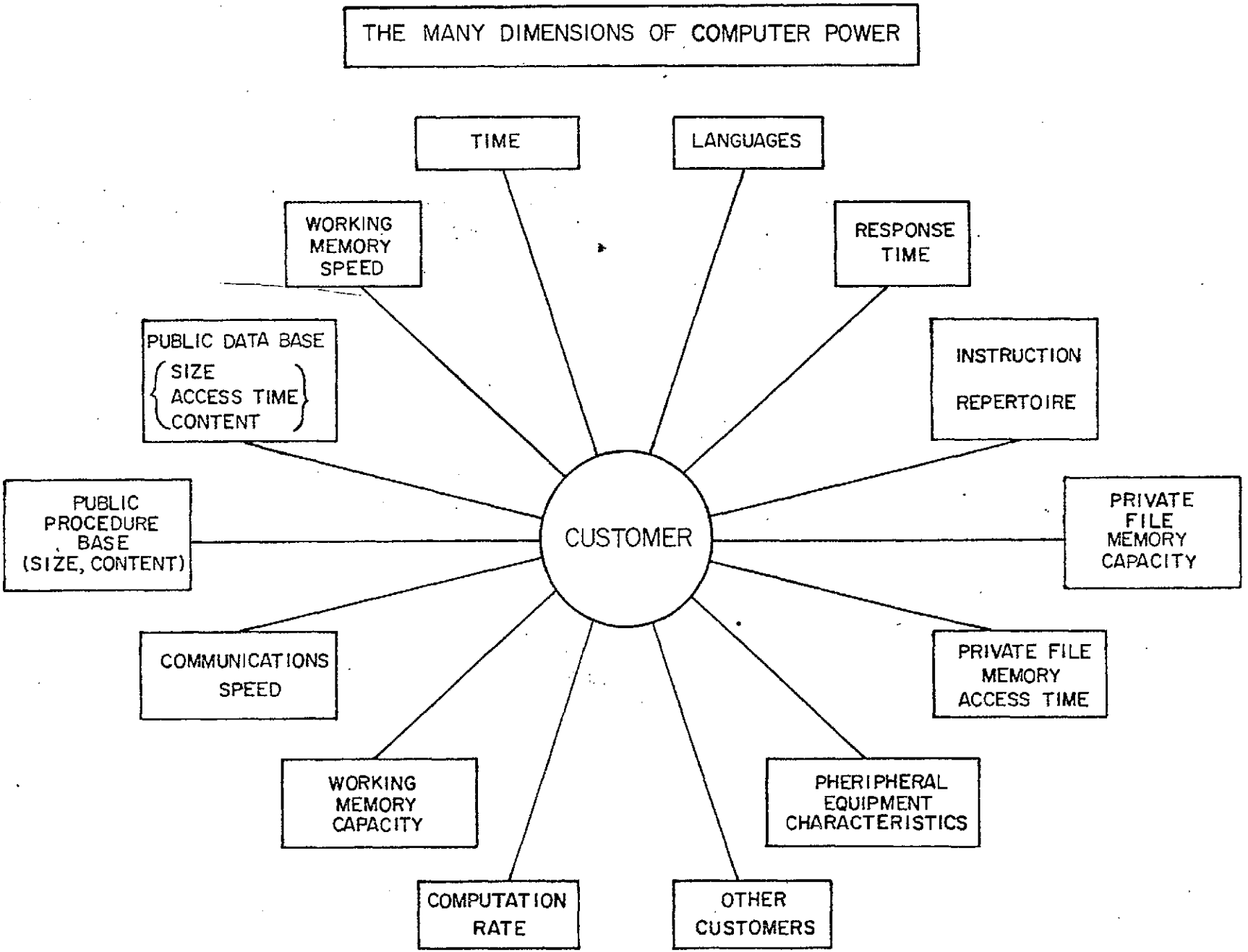

THE MANY DIMENSIONS OF COMPUTER POWER
TIME
LANGUAGES
WORKING MEMORY SPEED
RESPONSE TIME
PUBLIC DATA BASE
SIZE
ACCESS TIME
CONTENT
INSTRUCTION REPERTOIRE
PUBLIC PROCEDURE BASE (SIZE, CONTENT)
CUSTOMER
PRIVATE FILE MEMORY CAPACITY
COMMUNICATIONS SPEED
PRIVATE FILE MEMORY ACCESS TIME
WORKING MEMORY CAPACITY
PHERIPHERAL EQUIPMENT CHARACTERISTICS
COMPUTATION RATE
OTHER CUSTOMERS

FIGURE 2

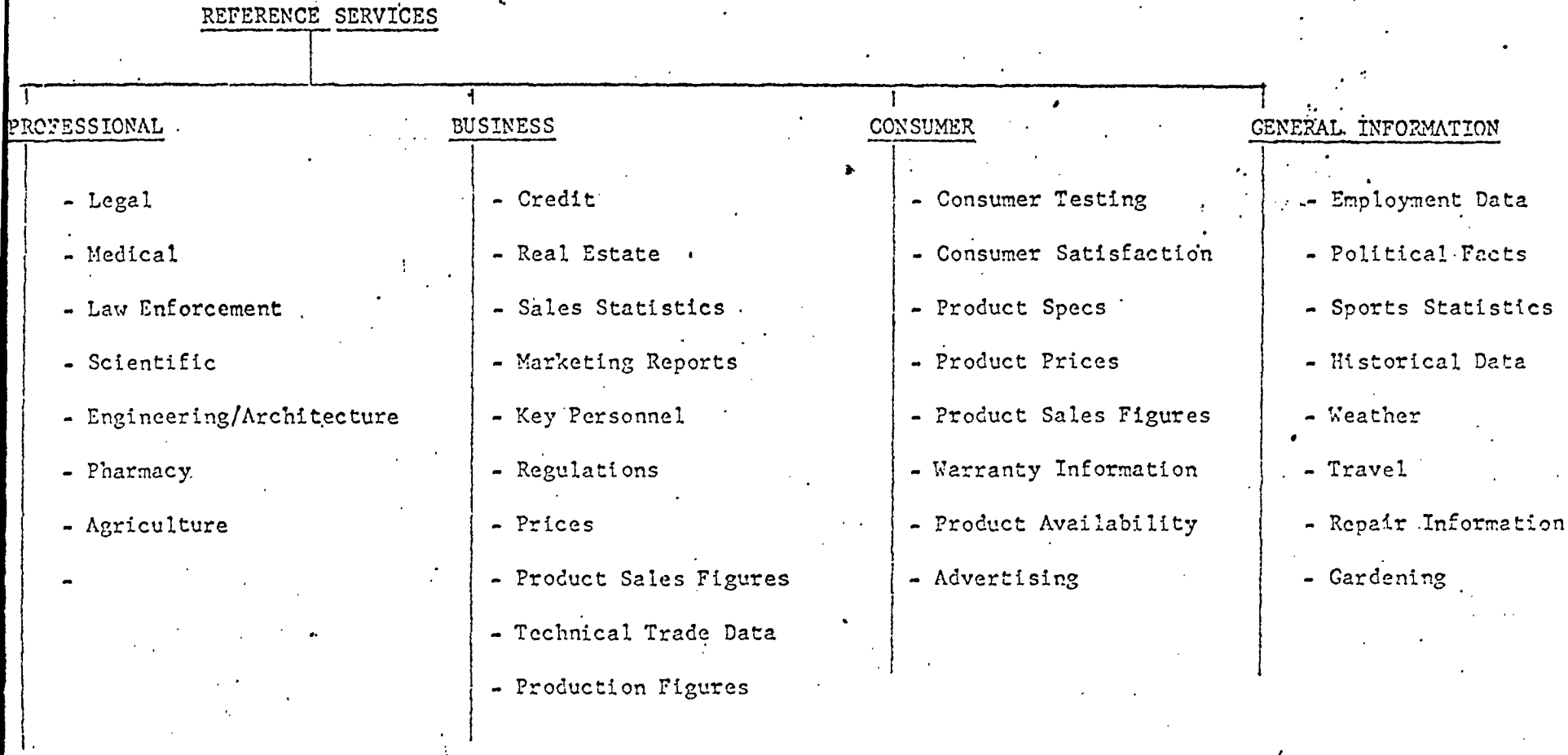
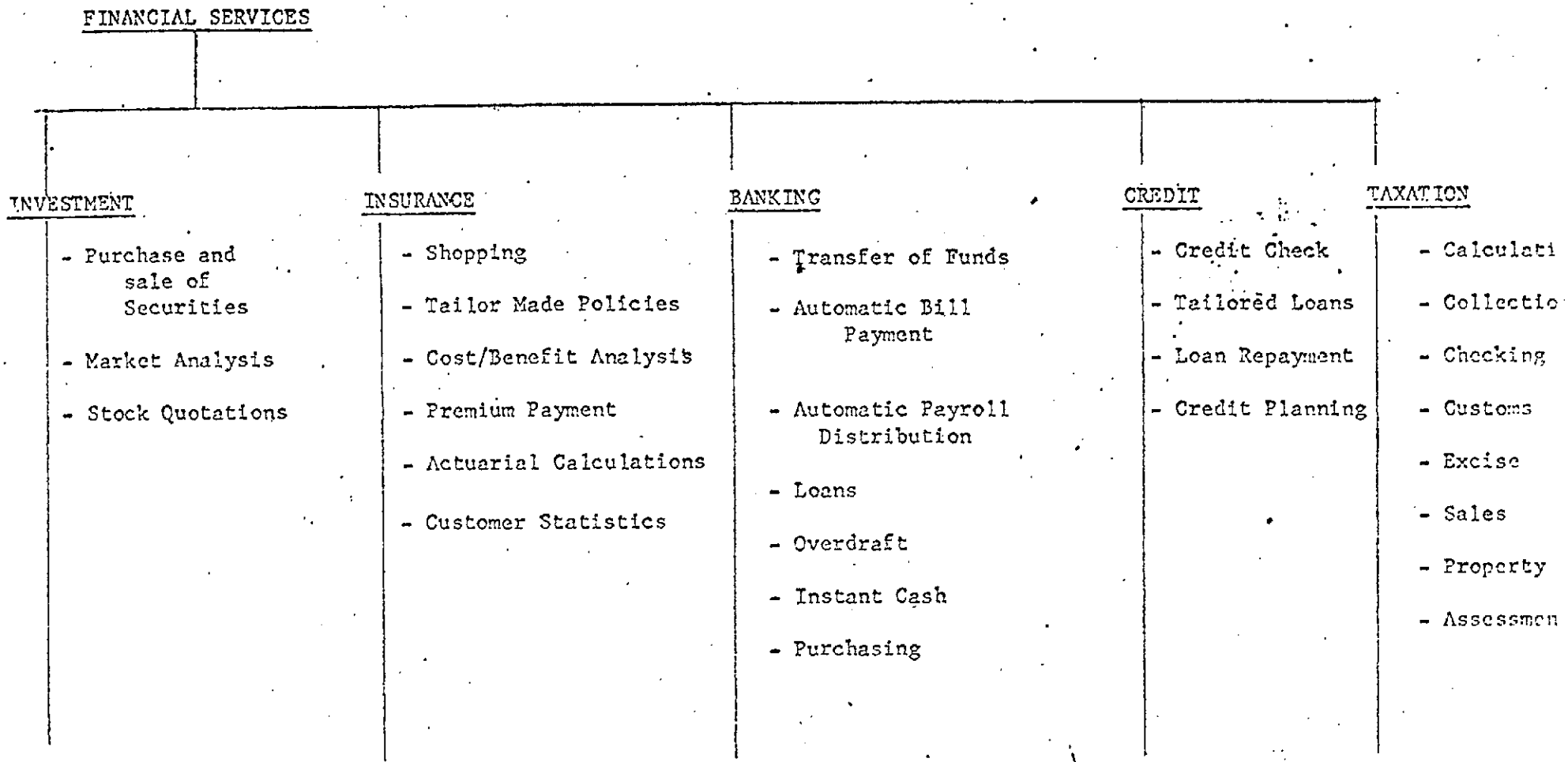

REFERENCE SERVICES
PROFESSIONAL
- Legal
- Medical
- Law Enforcement
- Scientific
- Engineering/Architecture
- Pharmacy
- Agriculture
-
BUSINESS
- Credit
- Real Estate
- Sales Statistics
- Marketing Reports
- Key Personnel
- Regulations
- Prices
- Product Sales Figures
- Technical Trade Data
- Production Figures
CONSUMER
- Consumer Testing
- Consumer Satisfaction
- Product Specs
- Product Prices
- Product Sales Figures
- Warranty Information
- Product Availability
- Advertising
GENERAL INFORMATION
- Employment Data
- Political Facts
- Sports Statistics
- Historical Data
- Weather
- Travel
- Repair Information
- Gardening

FIGURE 3


FINANCIAL SERVICES
INVESTMENT
- Purchase and sale of Securities
- Market Analysis
- Stock Quotations
INSURANCE
- Shopping
- Tailor Made Policies
- Cost/Benefit Analysis
- Premium Payment
- Actuarial Calculations
- Customer Statistics
BANKING
- Transfer of Funds
- Automatic Bill Payment
- Automatic Payroll Distribution
- Loans
- Overdraft
- Instant Cash
- Purchasing
CREDIT
- Credit Check
- Tailored Loans
- Loan Repayment
- Credit Planning
TAXATION
- Calculati
- Collectio
- Checking
- Customs
- Excise
- Sales
- Property
- Assessmen

GENERAL BUSINESS SERVICES

RETAIL & WHOLESALE PROCESSING

- Invoice Preparation
- Merchandise Management
- Credit Checking
- Point of Sale Recording
- Marketing

PRODUCTION CONTROL

- Scheduling
- Process Control
- Production Reporting
- Inventory Control
- Materials Management
- Resource Allocation
- Project Status Reports

PURCHASING

- Shopping
- Selling
- Ordering
- Payment
- Consumer Satisfaction Survey

PLANNING

- Sales Forecast
- Policy Selection
- System Evaluation
- Market Analysis
- Production Planning
- Investment Analysis
- Plant Layout
- Resource Allocation

MANAGEMENT INFORMATION

- Personnel
- Financial Reports
- Sales Reports
- Production Reports
- Inventory Status
- Market Situation

FIGURE 5

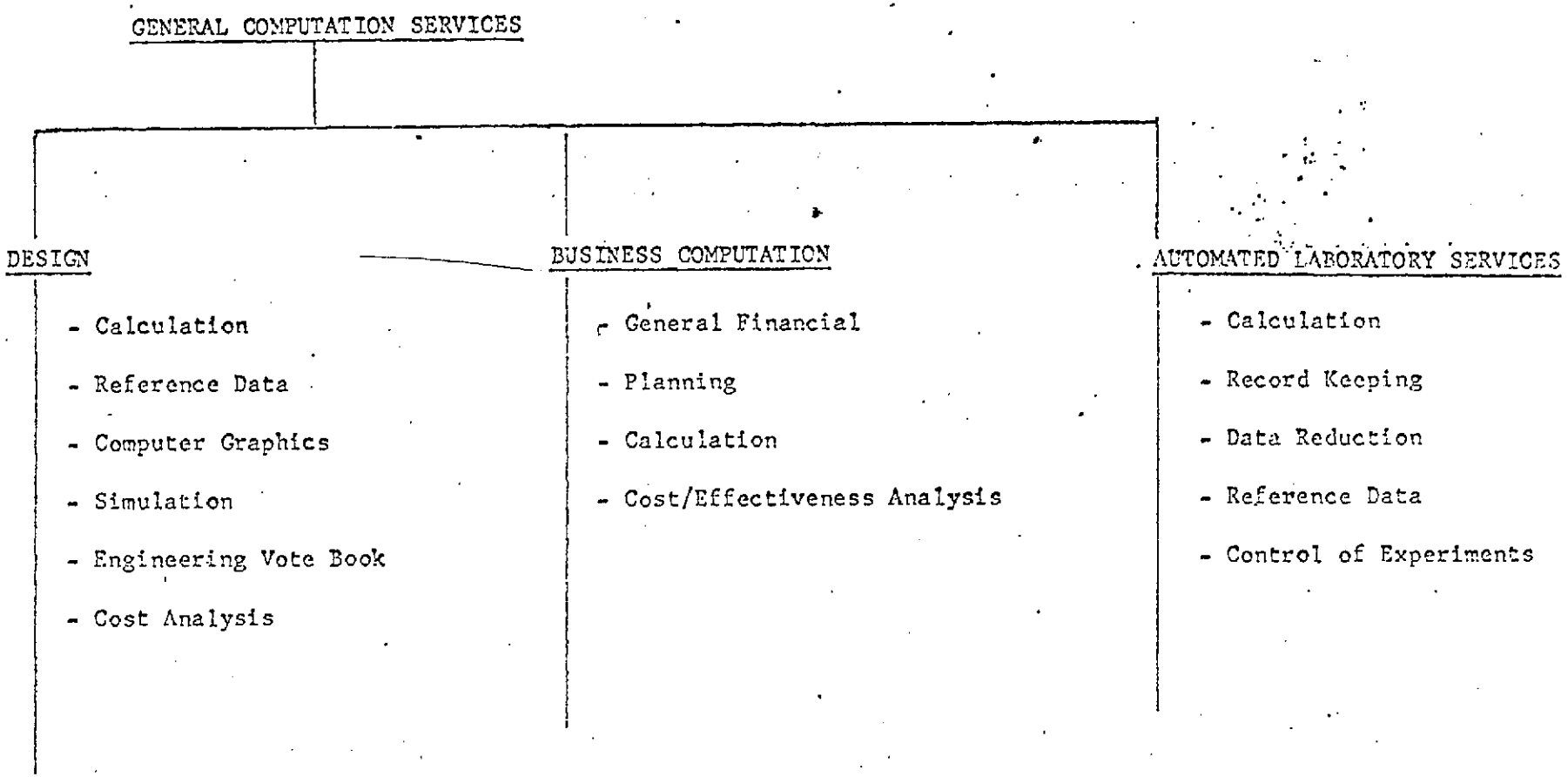
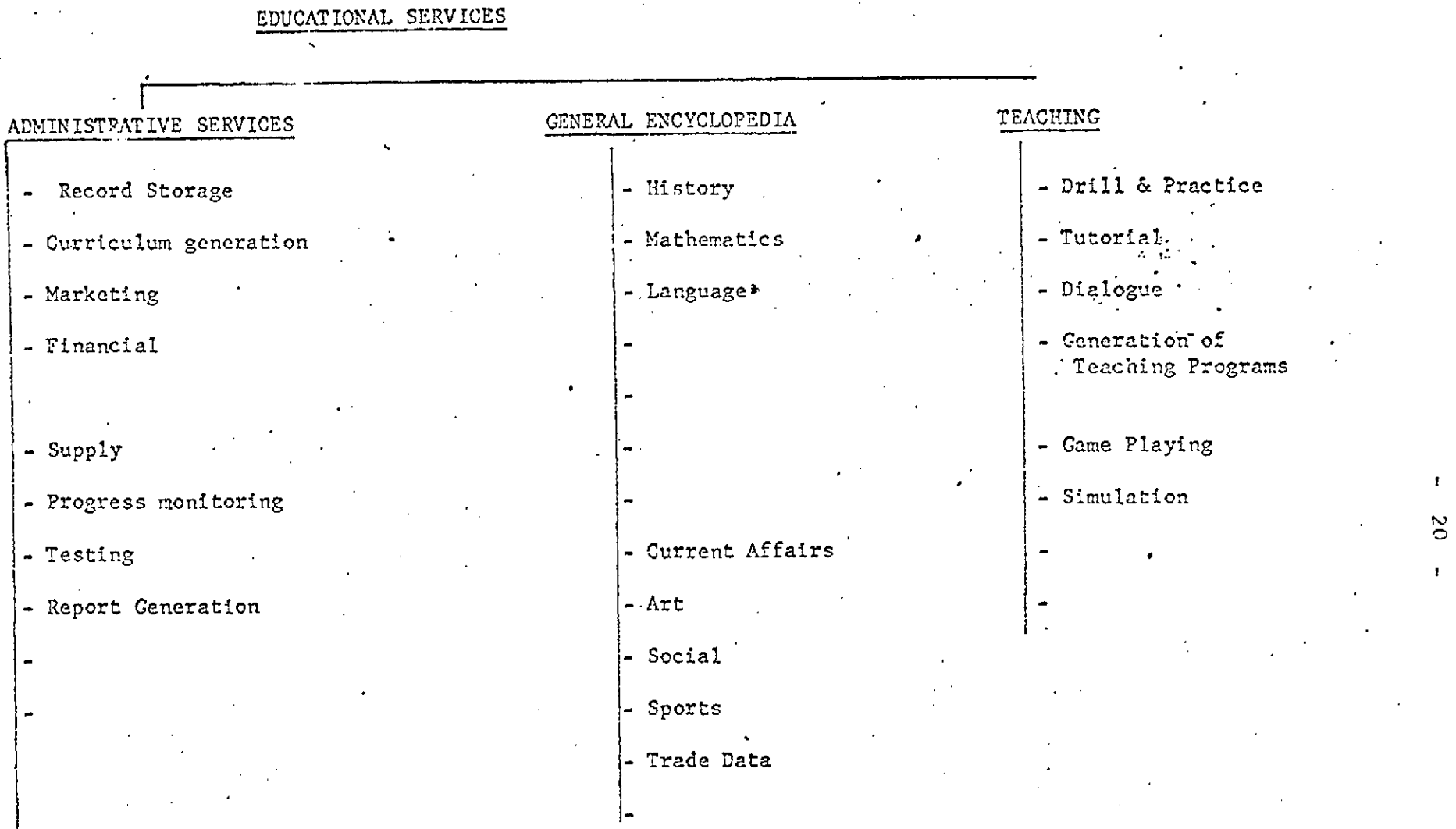

GENERAL COMPUTATION SERVICES
DESIGN
- Calculation
- Reference Data
- Computer Graphics
- Simulation
- Engineering Vote Book
- Cost Analysis
BUSINESS COMPUTATION
- General Financial
- Planning
- Calculation
- Cost/Effectiveness Analysis
AUTOMATED LABORATORY SERVICES
- Calculation
- Record Keeping
- Data Reduction
- Reference Data
- Control of Experiments

FIGURE 6


EDUCATIONAL SERVICES
ADMINISTRATIVE SERVICES
- Record Storage
- Curriculum generation
- Marketing
- Financial
- Supply
- Progress monitoring
- Testing
- Report Generation
GENERAL ENCYCLOPEDIA
- History
- Mathematics
- Language
- Current Affairs
- Art
- Social
- Sports
- Trade Data
TEACHING
- Drill & Practice
- Tutorial
- Dialogue
- Generation of Teaching Programs
- Game Playing
- Simulation

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 4

Privacy versus Freedom of Information

by

Hugh Lawford

Queen's University

CONFERENCE

SUR

L'ORDINATEUR, LA VIE PRIVEE ET LA LIBERTE D'INFORMATION

UNIVERSITE QUEEN'S

21-24 MAI

1970

RESUME

Privacy versus Freedom of Information

by Professor Hugh Lawford

Faculty of Law, Queen's University

The purpose of this paper is to suggest that Canadians should think carefully before adopting a general set of rules which give government the power to control how information can be collected and verified and to whom and under what conditions information can be transmitted. Broadly, this paper contends that attempts to protect a previously unrecognized right of privacy may erode a more fundamental right of freedom of speech and may interfere with a basic need for openness in the conduct of government and other institutions. The paper argues that the desire to protect privacy distracts us from the much greater danger which the computer brings -- the creation of a closed society where information falls under rigid controls. The paper urges that no action be taken to enshrine a legal right of privacy unless an overriding right of freedom of information is provided by law.

Privacy versus Freedom of Information

by Professor Hugh Lawford

Faculty of Law, Queen's University

The idea that the computer endangers privacy has led to a surprising reaction from the computer community, the general public and even the government. Computing Centre directors who have steadfastly denied that the computer is a suitable device for information retrieval nevertheless can see clearly that computerized information systems are a menace. Letters to the editor and the editorial column warn that human privacy is threatened. Fortunately, although information systems are complicated and incomprehensible, anyone can see that they may destroy privacy. And because the general public has recognized a danger, the government has not been slow to follow.

One could develop an argument that the infant information systems are too young to bear the burden of regulation. But that would be another paper. This paper argues that a single-minded concentration upon regulating the computer's impact on privacy distracts us from the

greater danger of the computer's impact on freedom of information.

Privacy and Free Speech

Many of the proposals for legislation concerning privacy assume that privacy is a fundamental human right. From the notion that privacy should be regarded philosophically as necessary for individual dignity and freedom, many persons assume that this social good should become a basic legal right.

Yet one can find very little in our common law tradition to support the existence of a legal right of privacy. If privacy is to be protected, legislation will be required. Our traditional common law rights seem inadequate to protect privacy.

If privacy is such a fundamental philosophical right, why has our common law system failed to develop a legal right of privacy? As Professor Gotlieb points out, the computer merely compounds or makes more obvious a problem inherent in information systems which are not computerized. Almost any organized system of gathering information brings together scattered items of

information about individuals into a revealing totality. Although this problem was not so grave before the computer arrived, the problem certainly existed. Why did the common law fail to develop the right of privacy?

Clearly the common law has been reluctant to recognise a right of privacy because such a right would endanger a more fundamental right of freedom of 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. Again, claims by Ministers of the Crown that they can refuse to testify about confidential government communications have been restricted by the courts. The courts have rejected claims to shelter whole classes of information and which have insisted that a judge has the power to look into the reasons for a claim of privilege. Yet again, rules of evidence which restricted the right of judge or jury to consider written or verbal communications gradually have been softened so that more evidence comes before the court. Arguments by doctors,

newspaper reporters and others that their professional ethics should give them the right to protect confidential communications have regularly been rejected and even the lawyer's right to protect communications from his client has been confined to communications for the purposes of litigation. In short, the law has been reluctant to restrict access to information. Even in cases where a need to protect confidences has been established, the law has controlled this protection closely.

Although it is unfashionable in some university circles to defend traditional liberal freedoms such as freedom of speech, I believe that most Canadians would agree that the way our law has developed has been the correct one. The keystone is freedom of speech and we should continue to require that those who wish to restrict this right must establish strong grounds for a restriction. Where a conflict arises between the right to free speech and another right, we should maintain our bias in favour of freedom of speech.

Openness in Government

Our Parliamentary democracy rests upon the basic rule that the people, if they become dissatisfied with

the conduct of government, may vote to replace it with another government. The intelligent operation of this system must require that the people have the ability to discover how their government is performing. Yet, ironically enough, the ability of Canadians to know what their government is doing depends to some extent upon the inefficiencies of the present government information system. Because many important documents must be circulated within the government itself, copies of such documents are printed or reproduced and some of these find their ways into the hands of the press or of the public. So long as multiple hard copies of a document are brought into existence, there is a good chance that the public will obtain access to the document -- or at least, that the file copy of the document will ultimately find its way into an archive to which a sufficiently interested person may obtain access.

Even if the existing system worked as it was intended to work -- even if every classified government document was seen only by officials with proper security clearance -- even if no government documents were ever "leaked" to sympathetic journalists by a minister, a member of a minister's staff or official -- the public interest in open government still would be protected by

the fact that the internal government community is large enough to provide some kind of public scrutiny of government documentation. Perhaps there is even an occasional official who considers that the document he is drafting may find its way into the archives and eventually be subjected to a critical or favourable scrutiny.

In short, the present system of handling government documentation carries with it the possibility -- indeed even the probability -- that enough important documents will sooner or later come into the possession of the public so that the nature of the process by which important government decisions are reached will be made known.

The computer changes all this. 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 names 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. One of the major reasons for creating an automated system is to reduce the human costs of maintaining files and libraries. But this saving involves the departure of the conscientious librarians and archivists who grasp government documentation and defend it from destruction. That is, an automated system makes redundant a whole class of human officials whose function has been to protect and preserve (and incidentally to scrutinize) government documentation.

The computer permits the creation of a system in which access to government information can be rigidly controlled and usage of government information can be strictly monitored.

Moreover, even if the computerized system is designed to transfer dead files automatically to some dead storage medium -- and one may suspect that it will be more likely that the system may simply erase dead documents -- the ability of the casual researcher to find particular documents will be far more limited.

Other Pressures Toward Closure

Economies of scale will tend to promote concentrations of information handling. Because major information systems are extremely costly, only governments or the largest corporations will be able to afford to create the systems. Even the privately developed systems probably will require extensive government funding, with the possibility of government participation in their administration. There are signs that advanced thinkers in the Federal government foresee the possibility of developing national information utilities, providing an integrated system through which a great variety of information may be offered to Canadians through an extensive network of computer terminals.

Already information has become much more of a commercial commodity than in the past. Publishers and

others can see that a computerized information system can provide a unit charge for every use of a document. Rather than a one-time recovery of a royalty or a profit from the purchase of a published book, the computer system permits a continuous collection of royalties and profits over a more extended period of time.

This possibility of substantial profits from marketing information pushes information systems in the private sector, and even in government, to impose controls on access to the information.

In sum, the computer almost certainly will result in the gathering of more information but in more controls of access to such information. The major problem of information systems will not be to protect the information from excessive disclosures, but to insure that the information is disclosed upon reasonable terms or even disclosed at all.

A Freedom of Information Act

Probably because of the existing bias of so much o our law toward freedom of speech, we have never enac detailed legislation to provide for a right of acces

information -- even to information under government control. Since research depends upon obtaining access to relevant documents, the difficulties of obtaining access have produced continuing friction between university scholars and government officials. Professor McPhail's concern lest new laws protect privacy, but inhibit research by social scientists, is another aspect of the general problem of scholarly access to information. Perhaps the advent of computerized information systems makes it necessary to review what rights we have to access to government information and to consider whether some specific law is needed.

Unlike a number of other governments, the Canadian government has never spelled out fully the terms on which its documents can be used. Canada has never enacted a clear law respecting clearance of documents and access to unpublished documents. Although Canada has established a national archives collection and has staffed these Public Archives with scholarly and helpful officials, the rules governing access even to the archives have been left vague and apparently arbitrary. Although the Public Archives Act provides for the transfer of records from the custody of various government departments into the archives and for the acquisition of other documents by

the Dominion Archivist, the act fails to make any provision governing conditions of access to the documents. Unlike the legislation in Great Britain, the Canadian act fails to confer any right to use or to copy any documents in the archives.

In fact, although the Public Archives Act seems to contemplate that orders in council will be passed respecting the custody of certain documents, no order in council appears to have ever been made under the act. If there are such orders in council, they have not been published as required under the Regulations Act. Since it is common knowledge that many government files have been transferred to the archives, one must guess at the authority by which the transfer was made. And more important, Canadians must guess about which documents have been transferred and what conditions have been attached concerning access to the documents transferred.

If there is no law giving Canadians the right to inspect government documents in archive collections, there is very little law or even policy on access to current material still in the possession of government departments or agencies. Some documents are treated as "public documents" and made freely available for

inspection. However, these documents tend to be a fairly limited group of formal papers, such as appeals to administrative tribunals. Once one moves beyond this limited group, almost all departments and agencies regard their files as closed to persons who are not public servants. Occasionally, a trusted scholar is permitted to see a particular set of files - normally on the condition that no material from the files is to be quoted without official approval. 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. Although Professor Donald C. Rowat of Carleton University has reported that there is a Treasury Board minute which requires that a department must secure permission from the Dominion Archivist if it wishes to withhold documents longer than 35 years, Treasury Board minutes, unlike orders in council, are not published in the Canada Gazette and distributed to depository libraries. Perhaps it is typical of our Federal government's attitude to information that the rule governing access to government documents is in itself inaccessible.

By comparison to the Canadian system, other governments state their rules governing access to documents in clear language in readily available laws. The British Public Records Act contains an express 30 year rule for access to documents. The Act states that the public has a right of access to the documents and requires an official to provide reasonable facilities to the public for inspecting and obtaining copies of the public records. The Act indicates a procedure by which permission can be given for access to documents less than 30 years old.

Sweden provides within its Constitution that every Swedish citizen has a right to free access to official documents. The limits on this right of access required by such matters as state security, diplomatic negotiations or police investigations are stated in the Constitution and are clearly defined in a special statute.

The United States too is far more open and liberal than Canada in making government documentation available. Under the pressure of an exceptionally vigorous and enterprising press and a traditional emphasis on openness in government, the United States permits individual departments and agencies to make their own rules about access. Although there is a 50 year rule governing materials deposited in the National Archives, the practise of the departments and agencies has been to set much shorter periods. For example, the United States State Department has the 30 year rule, but permits anyone demonstrating a legitimate need for the information to go back a further 10 years.

Even this rule has been regarded by Americans as too rigid. In 1961, President Kennedy advised members of his Cabinet that, "In my view, any official should have a

clear and precise case involving the national interest before seeking to withhold from publication documents or papers 15 or more years old."

An even more important development in the American system was the enactment in 1966 of the Freedom of Information Act. This new law gives an American citizen the right to obtain information from an agency and gives him the power of enforcing this right by court action. The key policy of the Act is that disclosure is made the general rule rather than the exception. All individuals are given equal rights of access to government information. The burden is placed upon government to justify withholding a document rather than upon the citizen to justify obtaining the document. And the cases in which documents are not to be available to the public are stated specifically and narrowly.

Clearly, if Great Britain, and Sweden, and the United States have all been able to provide by law for rights of access to government documentation, Canada should be capable of making a similar provision for Canadians. Fortunately, the enactment of legislation to protect privacy will provide an opportunity for enacting the more important rules to protect freedom of

information. No legislation should be enacted to protect privacy without such legislation to protect freedom of information.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 5

Professional and Technical Means of Reaching Objectives

by

J. M. Russell

Systems Dimensions Limited

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

CONFERENCE ON COMPUTERS:
PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY
May 21-24, 1970

PROFESSIONAL AND TECHNICAL MEANS OF REACHING OBJECTIVES

J.M. Russell
Vice President, Research & Development
Systems Dimensions Limited
Ottawa, Ontario

TABLE OF CONTENTS

A. Assumptions

This paper, having of necessity been prepared in advance of the Conference, was written from the point of view that several specific objectives would be generally agreed upon by the Conference attendees. The assumed objectives are:

1. That the rights of the individual pertaining to the scope, quality and distribution of personal information will be recognized and enforced by legislation; and

2. That computers are to be employed as the technical means of storing and controlling this personal information.

B. Professional Means of Reaching Objectives

1. Professional Requirements

Four distinct professional requirements would exist should we go forward with computerized databanks of private information.

First, would be the requirement for expert legislative draftsmen. Their job would be to draft practical legislation that would empower databank administrators to function and, at the same time, to establish appropriate safeguards of the individual's privacy.

Second, would be the requirement for information systems engineers of the highest calibre to both design and implement the computer systems to do the job. Since system capacity and data security constraints will be more stringent than ever before experienced together in the Canadian computer field, analytical planning and proven innovative skills will be at a premium. There will be little room for application of the scientific method of experimentation and observation.

Administrative professionals will be required to provide continuing administrations of these databanks. Since the formation of such databanks will necessarily span both changing public attitudes and continuously evolving computer capabilities, administrative professionals will require both flexible diplomatic skills coupled with sophisticated lay appreciation for computer capabilities.

The fourth professional requirement will be for those

who staff the regulating and appeal bodies. Personnel of these bodies will be charged with responsibilities to continuously re-interpret and re-apply legislature to changing times while guaranteeing the privacy of the individual.

2. Sources of Professional Personnel

Let us briefly examine the possible sources of such professional expertise in the light of their respective environments and presumed motivations.

Concerned legislative draftsmen can be expected to come forward from the legal profession and from all three levels of government: municipal, provincial and federal. The bar associations will be seeking justice in the form of enforceable regulations. Governments at all levels will be seeking control of the databanks, the administrative efficiencies afforded by their consolidation and the improved economic forecasting enabled by their analysis.

Candidates for the second professional group, the information systems engineers, will mainly be drawn from two levels of government, the universities, the private sector and, more specifically, the computer industry itself. Many federal government departments, several crown corporations and many provincial government agencies have for some time now 'een maintaining large files of the personal nature under discussion. To a much lesser extent, the universities have developed databanks. Perhaps the most expert, however, at interfacing the computer databank with the public are those members of the private sector that deal directly with the consumer. These are the life insurance companies, the retail

stores, the mail order houses, and the finance companies to name a few. The average Canadian on record at DBS, the Department of National Revenue, the Canada Pension Plan, his Department of Highways and his Provincial Hospitalization Plan will also be on file with one or two mail order houses, two or three life insurance companies, an automobile insurance company, three or four retail stores, two or three oil companies, his bank and perhaps several credit associations or finance companies. Although individual private sector databank custodians may administer the records of fewer people than do the governments, the quality of their performance is nonetheless maintained by competitive pressure. The fourth source of computer expertise is the computer industry itself. The industry, consisting of manufacturers, importers, consultants and service bureaux, can claim no particular expertise in administering databanks; it has been and continues to be, however, an important source of seasoned professionals that move into the sectors previously mentioned.

Administrative professionals for the proposed databanks can be expected to come from two sources: the governments and private enterprises presently managing equivalent, if not automated, databanks.

3. Licensing of Computer Personnel

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 that 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 databank 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 interests could 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.

C. Technical Means of Achieving Objectives

1. Security

The security of private information within computer databanks depends on two major factors. The first is the effective security of the combined computer hardware, software, communications network and remote terminal complex. The second is the integrity of the personnel having privileged access to the complex. For the purposes of this section, I will disregard the latter which has already been dealt with.

Technically speaking, the security levels available at a price from today's technology are quite high. A good insight into the tricks of the trade is provided by Mr. Lance Hoffman's excellent short survey on the subject, which was published in the June, 1969 issue of Computing Surveys.

Definitely, the most effective of the security methods is the use of privacy transformations or, more simply, scrambling. Although Mr. Hoffman had dwelled mainly on the scrambling of input and output databank information, it should be noted that nothing in today's technology prohibits the scrambling of the entire databank. Since normal file maintenance operations on both sequentially organized and 'randomly' organized databanks involve a periodic regeneration of the file, it is quite inexpensive to periodically alter the basic scramble code. The time duration between rescrambling is, of course, a function of the "work factor" involved in decoding the cryptographically encoded databank. An extension of this safeguard would involve the use of two-keyed locks in the form of serially applied multiple transformations in which

input and output are transformed according to algorithms known only by one group and the master file records transformed to the common natural language state from the scrambled master file record according to an algorithm known only to another group. This type of file and coding, together with one-time only passwords, will ensure the security of data records even in the case of physical theft.

It is worthwhile noting that since the time of Mr. Hoffman's survey several information systems have come into general use that provide for the password protection of individual items within an individual's record. One such system is IBM's GIS which stands for Generalized Information System. GIS, in conjunction with a modified IBM System/360 Operating System, provides both file and data item security.

It is worth noting here that the administration of passwords and other authorizing instruments is a costly and time-consuming function which cannot be hurried. Draftsmen of legislature should therefore provide adequate statutory time delays between the application and the granting of authority to access a databank.

2. Databank Uses

At this stage in the discussion, an important distinction must be drawn between two major uses of databanks.

The first use, which I will term "specific", is the use of a databank for purposes of inserting, updating, reporting, or deleting the record of a private citizen (or perhaps corporate citizen). The second use, which I will term "statistical", is the use of several, many

or all of the individual records of the databank for purposes of economic analysis, market research, population anlysis, public health and the like.

The primary purpose of the databank, "specific" or "statistic" tremendously affects the technical means of its implementation.

3. Databank Capacity Limitations

Using currently available technology, no significant databank storage capacity limitations present themselves to the designer of an on-line information service. By on-line, it is meant that the information is available to the computer without human assistance. 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 provice for approximately 10,000 words pertaining to every man, woman and child in Canada at a capital cost of approximately 50¢ per person. This figure, of course, excludes the costs of creation, reporting, updating, etc..

Databanks may be stored far more cheaply than this if immediacy of access is unimportant. The above hypothetical file, for example, would be contained in approximately 25,000 reels of conventional computer tapes at a capital cost of less than 5¢ per person.

Although almost all "statistical" uses of the databanks under discussion lack the immediacy factor, many of the "specific" uses require immediate access. Examples of such "specific" use would include point-of-sale credit checks and automobile ownership determination.

4. Databank Access Limitations

In spite of their incredibly large data holding capacities, the mass storage devices attachable to today's computers lack an extremely important attribute; simultaneity of access. Devices such as those mentioned above can generally be interrogated by only one or two persons at a time. 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 databank access applications alone, motor vehicle registration, for example, could tie up the system completely (three million vehicles registrations spread over 300 days = 10,000 registrations per day or 1,000 registrations per hour).

By subdividing the databank information on individuals either regionally or by application type, this apparent systems bottleneck can be somewhat eased by perhaps one or at most two orders of magnitude.

The accessing of such databanks for statistical purposes is considerably more efficient since the individual data records are accessed one after another in their natural physical sequence. These statistical accesses would nonetheless interfere with whatever "specific" accessing operations were simultaneously preceding. Consequently, it would appear that statistical operations would be necessarily delayed for execution to weekends or holidays. Because of the wide variety

of statistical accesses required, it is clear that statistical processes carried out on the primary databank would be limited to the copying of information on to more readily processable tapes (thus multiplying security risks).

The copying process alone could take up to several hundred hours

5. Start-up Problems

Special attention must be given to the problem of establishing computer based databanks. To become useful to industry and government alike within a reasonable time frame, many databanks will be built from records previously maintained by hand. 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. Because transcribed records of an individual may not come in to actual use for months or years after the transcription, errors introduced at that time will tend to be difficult to right.

Consequently, an important criterion for the establishment of such databanks should be the requirement that meaningful specific use be male of each record within some reasonably short time interval, such as ninety days.

The transcription of manually filed records is extremely expensive compared to the subsequent storage and processing costs. In many cases, this cost alone could

prohibit the transcription. To help offset these costs, databank facility managers might naturally look for by-product returns such as selling the name of the individual to a direct mail advertiser. Although most individuals would object to their names being added to such lists without their permission, the exciting possibility exists of establishing, on an individual basis, personal identity advertising tariffs whereby the individual for a fee would allow his name to be used for purposes of direct mail advertising.

6. Central vs. Distributed Databanks

In considering the technical options available to the designers of databank facilities, it is interesting to examine the pro and con of central distributed databanks.

The principal benefit claimed for central databanks is undoubtedly the economic and social value of the correlation analysis most easily performed on such databank. Secondary benefits generally claimed are efficiencies due to hardware economies of scale, least-cost administration and minimal security exposure.

On the other hand, the principal benefit claimed for either the regional or the agency distributed databank is the higher quality of conversion from existing records and the presumably better appeal mechanism. Other benefits claimed for distribution of databanks are the improved likelihood of public acceptance and the assume availability of common-carrier communications facilities to speed entire databanks to the researcher's location for correlation analysis.

Let us examine these claims.

Correlation analysis for economic or social purpose is, in fact, easiest to conceive using consolidated personal records as input. As mentioned earlier, however, the analysis itself may frustrate all attempts to maintain the personal information it attempts to measure, because of the state-of-the-art physical accessing limitations. Even the centralized databank would, therefore, be available for sampling only at periodic intervals.

Cost attractiveness of the central databank due to actual hardware economies of scale may be insignificant relative to overall plant, administration and communications costs which are likely to total ten times the cost of the computing equipment itself.

Similarly, the inherent attractiveness of centralized administration and security exposure may wane in the face of additional costs associated with interfacing with an unco-operative or skeptical public.

Distributed databanks would undoubtedly be easier to introduce and would have fewer problems due to inaccurate transcriptions. They would, however, suffer from non-uniform administration which quite possibly could spawn future compatibility problems. Non-uniform appeal mechanisms could severely endanger the privacy rirhts of individuals moving from one region to anoth r.

As to the assumed availability of common-carrier communication facilities to speed entire databanks to any particular location for correlation analysis, consider the following simple 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 databank, 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!

D. Summary

1. The professional requirements to introduce, administer and regulate databanks containing personal information dictate the need for involved participation of mission-oriented individuals drawn from widely differing environments.

2. Personnel licensing should be considered an individual security problem handled in the conventional way rather than by the creation of a new professional association.

3. Current technology can guarantee security of private information within databanks and access networks subject only to failures dependent upon the integrity of a relatively few trusted individuals.

4. Current and emerging computer mass storage devices will be ample to hold either central or distributed databanks.

5. Present and emerging computer methods of accessing mass storage devices will be inadequate to provide access to primary databanks for any purpose other than low volume reporting and updating. Periodically derived files will be used for statistical analysis.

6. Initial databank creation will present great hazards to the individual because of the quality control problems in converting from present non-mechanized data sources. Conversion costs may be offset by benefits obtained as a by-product of the initial conversion of an individual's record.

7. Common-carrier communications facilities will not support the transmission of databank material beyond that associated with reporting and updating. Copies of distributed databanks will, however, be easily transportable by physical means within time frames acceptable to the analysts.

par
John M. Russell

Résumé

1. Les exigences professionnelles nécessaires au dépôt, à l'administration et la réglementation des centres de données concentrant des données d'ordre privé imposent des besoins en personnes consacrées à une tâche particulière provenant d'une grande variété de milieux.

2. L'accréditation du personnel devrait être considérée comme un problème de sécurité individuel que l'on traiterait d'une façon conventionnelle plutôt que faire l'objet de la création d'une nouvelle association professionnelle.

3. La technologie actuelle peut garantir la sécurité de données d'ordre privé dans le périmètre des centres de données et dans les réseaux d'accès à l'exception de fuites dépendant de l'intégrité d'un relativement petit nombre de personnes de confiance.

4. Les dispositifs de mise en mémoire à grande échelle présentement disponibles et les dispositifs futurs seront assez vastes pour retenir aussi bien les centres de données centralisés que les centres périphériques.

5. Les méthodes informatiques présentes et futures d'accès aux dispositifs de mise en mémoire à grande échelle seront inadéquates pour accéder aux centres de données principaux pour des raisons autres que des transferts peu fréquents et la mise au jour. Des dossiers secondaires seront utilisés périodiquement aux fins d'analyses statistiques.

6. La création initiale de centre de données représente pour l'individu un grand risque à cause des problèmes de contrôle de la qualité au cours de la conversion des données actuelles non-mécanisées. Les frais de conversion pourront être compensés par les avantages obtenus des sous-produits de la conversion initiale du dossier d'un individu.

7. Les moyens de communications des services publics ne pourront assumer la transmission du matériel des centres de données autre que celui visant à la mise à jour des données. Cependant, des examplaires des données des centres pourront facilement être transportés par des moyens ordinaires à l'intérieur de structures horaires acceptables pour les analystes.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 6

Computers-- Some Proposals for Legislation

by

Professor J.M. Sharp

University of Manitoba

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

COMPUTERS -- SOME PROPOSALS FOR LEGISLATION

A Paper Presented For The National Conference

By Professor J.M. Sharp

A Résumé

This paper makes recommendations on the assumption of jurisdiction and the passing of legislation to protect individual privacy in the face of ever-increasing computer operations.

It is suggested that the Federal government should create a task force to prepare legislation in those areas within Federal jurisdiction. A wide Federal jurisdiction could be assumed on the basis of

a) the "stream of commerce" doctrine,

b) the telecommunications analogy,

c) the criminal law and national security.

Only certain completely local computers with no international or inter-provincial links would fall outside this jurisdiction, and Provincial legislation (preferably uniform) could close any gaps thus left.

The legislative controls advocated in this paper include the creation of a licensing and regulatory scheme; this would demand the licensing of every data bank as a data bank, quite apart from other business licensing, etc. It is further suggested that the collection and storage of data be controlled by creating "restricted classes" of information, cut-off dates, so that "stale" information is not used to damage individuals, and regulation of links between data banks (particularly international links) and sale and disposal of information.

It is also submitted that an individual should, subject to certain restrictions such as Crown privilege, be able to receive a print-out of the record on him and demand rectification where errors are present.

The paper finally recommends the creation of the task force as a first priority.

LES ORDINATEURS: DE L'OPPORTUNITÉ DE LA LÉGISLATION

Conférence présentée devant le Congrès National
par M. le Professeur J. Sharp

La présente conférence considère quelle compétence doit être revendiquée et quelles dispositions législatives adoptées pour protéger l'individu contre la divulgation d'information le concernant, face aux opérations toujours croissantes des ordinateurs.

Il est suggéré que le gouvernement féderal mette sur pied une équipe chargée de la préparation des lois dans les domaines qui sont de la compétence fédérale. La compétence fédérale pourrait être élargie en se basant sur

a) la doctrine de la circulation du commerce;

b) l'analogie des dispositions en matière de télecommunication;

c) la lois pénale et la sûreté nationale.

Seuls certains ordinateurs fonctionnant sur un plan exclusivement local et sans contacts interprovinciaux ou internationaux échapperaient à cette compétence; et une législation provinciale; de préférence uniforme, comblerait toute lacune éventuelle.

Le contrôle légal recommandé au cours de cette conférence comprendrait un régime de réglementation, avec subordination de toute opération à l'obtention d'un permis: ce permis serait requis pour toute banque d'information en tant que telle, indépendemment de tout autre permis commercial. Il est en outre suggéré que la constitution de ces dossiers soit réglementée par la prescription de classes réservées d'information, de dates limite qui empêcheraient les informations périmées de porter prejudice a l'individu, par le contrôle des relations entre les différentes banques d'information, tout particulièrement les rélations internationales; enfin par le contrôle de la vente et de la cession de ces dossiers.

L'individu devrait aussi avoir la possibilité, sous réserve de certaines restrictions telle que l'immunité gouvernementale, d'exiger une copie integrale de son dossiere et de requérir la rectification des erreurs éventuelles.

En terminant il est recommande que la création de cette équipe ait entière priorité.

COMPUTERS - SOME PROPOSALS FOR LEGISLATION

A paper prepared for the national conference on "Computers - Privacy and Freedom of Information" by Professor J. M. Sharp, Director, Legal Research Institute of the University of Manitoba.

The purpose of this paper is to examine the legal and regulatory means of attaining objectives examined in detail by others in papers designed to precede this one. It is because the philosophical and conceptual considerations underlying the delineation of these objectives have been examined in these other papers that they are not here considered. The paper proceeds, however, on the a priori assumption that the two constituent elements which make up the title of the conference - namely, privacy and freedom of information - are inherently desirable ends, and that any legislative proposals must at least take account of, and, if possible, strike an acceptable balance between the two concepts.

The Standing Committee on Justice and Legal Affairs in its report to the House of Commons on March 11th, 1970, stated that,

> "If the flow of information held by or under the cognizance of the Government of Canada is to be formally restricted in any way by Parliament under the rubric of protection of privacy, then there is created a parallel need to define classes of information in which the public interest in freedom of communication outweighs the public interest in the restriction of access to or dissemination of such information on privacy grounds. Another extremely significant area lies in the interprovincial and international flow of personal information through telecommunications facilities linking computers with central data banks. No

> new development in trade and commerce has ever had more need for or been less subjected to regulation than the private data being programmed into and transmitted by such systems."[1]

This passage from the Report pinpoints an area in which the need for critical evaluation and regulatory action becomes daily more urgent.

Legislative Competence

Before any specific proposals may be advanced, the question of legislative and jurisdictional competence must be considered. 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 regulation. The computer which acts as a repository of information without either contributing to or drawing upon inter-provincial or international patterns of information flow, but supplying only intra-provincial sources of demand is a different creature for jurisdictional purposes, as indicated below.

Several grounds may be advanced in support of a federal assumption of jurisdiction in this area. These include:

1. The "stream of commerce" doctrine

The assumption of federal jurisdiction on the basis of this doctrine alone is, perhaps, of conjectural validity, or acceptability. The doctrine - and the metaphor inherent in it - has been subjected to considerable criticism, primarily by academic writers. Notwithstanding these attacks, however, the Supreme Court of Canada has utilized the doctrine at least twice in strongly assertive terms in recent years. In Reference Re the Farm Products Marketing Act,[2] the Chief Justice of the Supreme Court declared that "once an

article enters into the flow of interprovincial or external trade, the subject matter and all its attendant circumstances cease to be a matter of mere local concern." Again, in the more recent decision in Canadian Warehousing Association v. The Queen,[3] Pigeon, J., in delivering the judgment of the Court lent considerable credence to the doctrine as a viable concept. It is, of course, quite feasible that federal jurisdiction may be asserted on this basis, but the fact remains that it is far from being the ideal foundation on which to build a new legislative edifice, and perhaps questionable whether Canada would wish to elevate it (to mix the metaphors) to the position it occupies in the United States of America. As one writer on the American experience has recently commented,[4] "commerce, or more accurately, the federal government's power over commerce, is now clearly a brooding omnipresence within as well as without the borders of each state, and its mere invocation by Congress is sufficient to call forth a policy of judicial restraint in the examination of both the wisdom and the power of the federal government to enact legislation pursuant thereto." Caution over the creation of a similar jurisdictional climate in Canada might result in a rather circumspect approach to the actual grounds for assumption of jurisdiction. This would require examination of the following, alternate bases.

2. The telecommunications analogy

The Telesat Canada Act of 1969[5] incorporated a federal company whose objects[6] are expressed to be "to establish satellite telecommunication systems providing, on a commercial basis, telecommunication services between locations in Canada". Section 9 of the Act provides that the company "shall

not, except under the direction of the Minister, directly or indirectly negotiate or enter into an arrangement or agreement with a foreign state, an organization composed of representatives of foreign states or a corporation acting as an agent for or on behalf of a foreign state".

The connection and similarity between a telecommunications system and a network of inter-connected computers and data banks hardly needs stressing, particularly as "telecommunication" is defined, for the purposes of the Telesat Canada Act, as "any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system".[7] In the Act, the Federal authorities have not only moved firmly to establish federal jurisdiction and control over an area for which the creation of one unified legal régime is of paramount importance, but have recognized also that some aspects of the matter, especially those involving international considerations, demand governmental participation, as through such provisions as section 9.

While it is not argued that the creation of a public corporation along the Telesat lines is necessarily the model for the regulation of flows of computerized information, it is submitted that the concept which underlies what has been done in this instance in terms of assumption of jurisdiction bears both substantive and intuitive comparison with the considerations involved in the regulation of linked computer operations.

3. The Criminal Law and National Security

Two other sources of federal legislative competence may be referred to as supplementary, rather than primary, arguments. The federal power to enact criminal laws is obviously relevant in this field, but can provide only partial solutions. It is one thing to prohibit and take criminal sanctions

against particular uses and abuses of computer facilities; it is quite another to produce a comprehensive scheme of things which will set out not only to eradicate such abuses, but to compensate also the hapless victim when such an abuse does take place and does damage an individual.

This is one problem which, incidentally, faced the Standing Committee of the House of Commons on Justice and Legal Affairs, which considered the matter of wiretapping. Amendments to the Criminal Code could clearly provide criminal sanctions against prohibited uses of wiretaps, but here again the fact was faced that the federal jurisdictional power did not extend (under the present law) to provide compensatory tort remedies for the injured individual.

The criminal law is, therefore, perhaps not the vehicle to deal with all aspects of computer regulation. It remains, however, a useful weapon in the federal jurisdictional armoury in this area.

National security is the last factor referred to under this head - again as a supplementary, rather than primary, point. The creation of a system of linked data banks in Canada would inevitably involve international flows of information. To expect credit, commercial and other information to move only in a back and forth East-West flow within Canada is to ignore reality. One instant reality is a North-South and vice versa flow, and in due course extra-continental flows will also develop. As a result, foreign intelligence systems (state, industrial or commercial) might tap a U.S. data bank and gain data on Canadian individuals, firms and the Canadian economy. A real question of national security could arise in this area, and the federal government would clearly then have jurisdictional competence to control content and output from the system. This

would apply in principle to any system in which there is an interchange with any other country.

To summarize these remarks on legislative competence, there seems to be several sound justifications for a federal rôle in regulation and control. This applies particularly to an inter-provincially or internationally operative system. The non-linked data bank, as suggested below, should be subjected to certain controls, and provincial legislation (ideally in the form of a uniform statute) would be needed to effect this. 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 inter-locking system of federal-provincial legislation should not be evolved to deal with data banks and the information they store.

Legislative Controls

One writer recently commented that "the efforts of the computer industry to provide for security technology have thus far been minimal, but the potential for protection circuitry is high. Proposed methods for protecting computer records from surreptitious access include: cryptography in transmission of data; scrambled storage formats; random external auditing of record use and program alterations", etc.[8]

Useful though these technical safeguards may be, there can be no confident regulation of input, storage and outflow of data, and the best good will in the world of the operators of data banks cannot guarantee security of privacy, without legal sanctions to lend "teeth" to the good intentions.

It is for this reason that the following legislative proposals are advanced, bearing in mind that any individual proposal might have to be reproduced on with the federal and provincial levels in order to provide a "watertight" system.

1. Licensing and Regulatory Scheme

The creation of a licensing scheme is fundamental; without it, enforcement of the following proposals would be difficult, if not impossible. The concept of licensing in the information storing and retailing world is not new. As an example of licensing in the general area, reference may be made to the Ontario Private Investigators and Security Guards Act, 1965;[9] this requires the licensing of "private investigators", defined as "a person who investigates and furnishes information for hire or reward, including a person who searches for and furnishes information as to the personal character or actions of a person, or the character or kind of business or occupation of a person . . ."[10] Under the Act the post of registrar of private investigators and security guards is created, and he is responsible for the licensing of and observance of regulations by these bodies and persons.[11] Certain classes of investigators are specifically exempted from the application of the Act.

It is 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. The licensing should be of the installations as data banks, even though the operator should be subject to licensing under general or provincial legislation for other purposes.

It is further suggested that at the federal level an independent Board or Commission be created, representative of as many substantially interested

sectors of society as feasible, which will then issue and administer regulations aimed at achieving the desired ends. On the provincial level, it might be possible to confer similar functions upon an existing suitable administrative machinery, although the source of regulations employed in the Ontario Act referred to above (the Lieutenant Governor in Council, Province of Ontario[12]) would not be advocated as the source of regulations for this purpose.

The advantage of the Board would be that regulations could be made expediently to distinguish between the types of information (e.g. truly private and what is adjudged to be "public") and the purposes for which any given piece of information may be used (e.g. governmental use and private commercial use). The law in this area would be developed much more quickly than if left to the Courts, and a member of the judiciary in any case could be Chairman or member of the Board.

2. Collection and Storage of Information

The regulations would have to make a qualitative assessment of what information may be collected and stored in certain data banks. Should it, for example, be lawful for unverified information obtained by interviewing a subject's neighbours to be stored permanently in a data bank or at all? Should a criminal record be stored for open access, or should it be stored with a precoding with the effect that that particular piece of information is thereafter or after a certain period of time only available to certain government departments? It is undoubtedly technically possible to create "public areas" and "restricted areas" within a memory bank by means of precoding which would require the requisite "key" to open the particular area for scrutiny. Such matters as details of certain notifiable diseases

might also justifiably be put on a restricted bases. It might even be desirable that certain facts should be available to some government departments but not to others. This could be equally achieved.

A somewhat related matter is that of "cut-off dates". While it may be argued 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.

Associated Credit Bureaus Inc. of Houston, Texas, in "Credit Bureau Policies to Protect Consumer Privacy" (policies, incidentally, substantially endorsed by the related Associated Credit Bureaus of Canada) lays down the following file retention procedures:

> "All procedures indicated in this section are stated in terms of length of time the specified items are to be reported. The intent is to insure the mandatory reporting of the specified items for the time periods indicated, and the discontinuance of reporting after such time periods have expired. Whenever it is ascertained that a specified item in the bureau file is to be reported no longer, such item is to be deleted from the file as soon as practical.
>
> 1. A credit bureau shall report bankruptcies of all types for not longer than 14 years from the date of adjudication of the most recent bankruptcy.
>
> 2. A credit bureau shall report records of accounts placed for collection and records of accounts charged to Profit and Loss for not longer than 7 years, or until the governing statute of limitations has expired (whichever is the longer period).

3. (a) A credit bureau shall report suits and judgments for not longer than 7 years from date of entry, or until the governing statute of limitations has expired (whichever is the longer period).

   (b) A credit bureau shall report paid tax liens for not longer than 7 years. But there is no limitation on reporting of unpaid tax liens, because of no statute of limitations on such items.

4. A credit bureau shall report records of arrest, indictment or conviction of crimes for not longer than 7 years from the date of release or parole. Such items shall no longer be reported if at any time it is learned that in the case of a conviction a full pardon has been granted, or in the case of an arrest or indictment a conviction did not result.

5. A credit bureau shall report any other adverse data not otherwise specified in this section for not longer than 7 years.

6. A credit bureau shall delete as soon as practical any item of derogatory information whenever it is ascertained that the source of information can no longer verify the item in question from its records of original entry."

Somewhat similar provisions are included in a Bill recently introduced into the U.S.A. Senate as an amendment to the Consumer Credit Protection Act, and referred to the Committee on Banking and Currency.[13]

Here again, precoding could render cut-off dates applicable to certain data-bank users and not to others so as to achieve a balance between the preservation of the public interest and the individual's privacy. A cut-off date would, therefore, not necessarily involve a total deletion of a given category of items from the memory bank unless this was deemed advisable by the Board.

As noted above, guidelines to govern file retention procedures have been evolved to deal with file-based data stores. It is strongly suggested that these be considered together with any proposals geared particularly

to computer operations.

3. Links between Data Banks and Sale of Information

Links between two or more data banks and links between data banks and terminals should be subject to the control of and the close scrutiny of the proposed Board, which should satisfy itself that the potential recipient of information, either for the purposes of swelling an existing memory bank, or for simple "retail use" is a reputable, responsible and acceptable repository or recipient. 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. In this connection, attention is drawn once again to the analogy of section 9 of the Telesat Canada Act.[14]

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. We have here a good example of the whole being much more than the component parts. Serious consideration should be given to whether a truly gargantuan memory bank should be allowed to develop.

Even within 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[15] 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.

4. A Right to Verify

Some thought may be given to the creation of a right in the individual, subject to certain limitations, to see, and if necessary demand the correction of, the data held on him in the memory bank. The data bank may, like the proverbial elephant, never forget and may never be faulted in its recollection - but what if it has been fed faulty information in the first place? The chance of human error in programming and feeding the memory may be small, but cannot be eradicated. This has been pointed out on a number of occasions, particularly in connection with the file operations of credit reporting agencies (where the incidence of error is small, but, in

the writer's view, none the less significant).

Some concerns (e.g. Associated Credit Bureaus of Canada) now follow guidelines which allow a person to enquire as to the contents of his file and thus be able to challenge the veracity of or request the amendment of any item.

In principle, there is no reason why the regulations made pursuant to the proposed legislation should not give individuals the right to acquire a print-out of the records held on them. Some restrictions upon this right must be acknowledged. 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. The regulations could determine a scale of fees. Again, certain types of information (e.g. that subject to Crown privilege, which would be only in a government data bank in any case, and that subject to other justifiable forms of privilege) could be kept out of the individuals print-out by precoding, again subject to rigorous controls to prevent "white washing".

This right, it is contended, is of importance.

5. Miscellaneous

Several other matters should be covered by the legislation or regulations. Attention might be given to licensing (and bonding) of those with access to data banks and terminals. Physical security measures could be stipulated. Procedures for disposal or destruction of records could be laid down. These are details which are important, but not matters of major principle, and therefore not considered here in detail.

6. Conclusions

The proposals advanced above are those which seem of prime urgency.

Time is not on the side of the legislators. Very recently, for example, The Credit Bureau, Inc., of Atlanta, Georgia, issued a booklet "C.B.I. Project 1970" describing how the files of credit bureaus over a large geographical area of the Southeastern U.S.A. are being computerized; the system will be fully operational by the end of this year, and at this rate a continental system, at least for credit data, could be created very speedily.

The final, and strongest, plea of this paper is that a task force be created without delay to tackle the problems outlined briefly above, and to propose legislation. This task force should be on a federal-provincial basis, and would undoubtedly achieve what twenty ad-hoc conferences cannot do. This fact is recognized in the Report on Protection of Privacy prepared for the Ontario Law Reform Commission by Professor E.F. Ryan.[16] If the problem is not tackled in its entirety, and soon, there will be little to do but sit back and observe the ultimate victory of machine over man.

J. M. SHARP

SUMMARY OF PROPOSALS

1. Assumption of jurisdiction by federal government over greatest possible number of data banks; complementary legislation (preferably uniform) on provincial level to plug gaps.

2. Creation of federal board to lay down regulations and administer legislation. Similar scheme in provinces, possibly using existing machinery where feasible.

3. Licensing of all data banks, and subjection to regulations.

4. Classification of information, and restrictions on release by use of precoding. Imposition of "cut-off" dates, achieved by precoding.

5. Control of links between data banks.

6. Control of output of information.

7. Creation of individual right to verify or seek amendment.

8. Miscellaneous provisions relating to licensing and bonding of employees with access, destruction or disposal of records, etc.

9. Creation of task force on federal-provincial basis to avoid disjointed, ad-hoc conferences.

FOOTNOTES

1. Minutes of procedings and evidence No. 7, Feb. 5, 1970, p. 7 - 41.
2. [1957] S.C.R. 198
3. (1969), 1 D.L.R. (3d) 501
4. Professor E. F. Ryan, (1969) 47 Can. B. Rev. 318, at p. 319.
5. Stats. Can. 1968-69, c. 51
6. Ibid., s. 5
7. Ibid., s. 2
8. Jeffrey A. Meldman, (1969) 52 Marquette L. Rev. 335, at p. 353.
9. Stats. Ont. 1965, c. 102
10. Ibid., s. 1
11. Ibid., s. 3
12. Ibid., s. 34
13. Committee Print No. 3, October 8, 1969.
14. Stats. Can. 1968-69, c. 51
15. Toronto Star, January 12, 1970
16. Ontario Law Reform Commission, 1968.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 1

Computers and Privacy: A Survey

by Lance J. Hoffman

an extract from "Computing Surveys", June 1969

*****

DOCUMENT NO 1

Computers and Privacy: A Survey

par Lance J. Hoffman

extrait de la revue "Computing Surveys", juin 1969

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

Computers and Privacy: A Survey

LANCE J. HOFFMAN

Stanford Linear Accelerator Center, Stanford University, Stanford, California*

The problem of access control and privacy in computer systems is surveyed in terms of existing systems and current proposals. A review of suggested legal and administrative safeguards is given. The bulk of the discussion deals with the current technology, its limitations, and some additional safeguards which have been proposed but not implemented. Finally, a few promising computer science research problems in the field are outlined. A partially annotated bibliography of literature in the area is included.

Key words and phrases: privacy, access control, confidentiality, privacy transformations, social implications, public utility, time-sharing, legislation, regulation, professionalism, access management, data bank, dossiers, ethics, authority items

CR categories: 2.11, 2.12, 2.2, 2.3, 4.30

THE PRIVACY PROBLEM

In the last several years, computer systems used as public utilities have moved from dream to reality. There are now a large number of multiterminal, on-line, time-sharing systems in both commercial and academic environments [13, 15, 42, 49, 50]. Many people fully expect a public "data bank grid" to come into existence in the very near future; they point out [47] that "it is as inevitable as the rail, telephone, telegraph, and electrical power grids that have preceded it, and for the same reasons. It is much less expensive and more efficient to share information than to reproduce it."

Unfortunately, current information networks do not have adequate safeguards for the protection of sensitive information. However, since the benefits derivable from automation of large data banks are so great, pressure in some circles [17, 20, 33, 34] is building up to "computerize now." Automation offers benefits in both economy and performance over many current systems.

* Computation Group. This work was supported by the US Atomic Energy Commission.

Social scientists and statisticians, for example, have suggested the creation and maintenance of a national data bank [34]. Its use would remedy many defects of current files and procedures which result in information unresponsive to the needs of vital policy decisions. Some of these defects, as pointed out by Dunn [21] are:

—Important historical records are sometimes lost because of the absence of a consistent policy and procedure for establishing and maintaining archives.

—The absence of appropriate standards and procedures for file maintenance and documentation lead to low quality files that contain many technical limitations in statistical usage.

—Many useful records are produced as a by-product of administrative or regulatory procedures by agencies that are not equipped to perform a general purpose statistical service function.

—No adequate reference exists that would allow users to determine easily whether or not records have the characteristics of quality and compatibility that are appropriate to their analytical requirements.

—Procedures for collecting, coding and tabulating data that were appropriate when developed now lead to some incompatibilities in record association and usage required by current policy problems and made possible by computer techniques.

—There are serious gaps in existing data records

CONTENTS

that stand in the way of bringing together records of greatest relevance for today's problems.

—The need to by-pass problems of record incompatibility in developing statistics appropriate for policy analysis, places severe strains upon regulations restricting the disclosure of information about individuals. Technical possibilities for using the computer to satisfy these statistical requirements without in any way violating personal privacy have not generally been developed and made available by the agencies.

To take advantage of the economies and capabilities of the computer, governmental agencies and private organizations such as credit bureaus are making use of computer-based personal dossier systems. The New York State Identification and Intelligence System (NYSIIS) provides rapid access to criminal histories, stolen property files, intelligence information, etc., for use by [26] "qualified agencies." Santa Clara (California) County's LOGIC system [17] will include a person's name, alias, social security number, address, birth record, driver and vehicle data, as well as other data if the person has been involved with the welfare or health departments, the district attorney, adult or juvenile probation, sheriff, court, etc. Other municipalities have created similar systems.

These large data banks will make it easy for the citizen in a new environment to establish "who he is" and thereby to acquire quickly those conveniences which follow from possession of a reliable credit rating and a social character acceptable to his new community. At the same time, commercial or governmental interests will know much more about the person they are dealing with. We can expect a great deal of information about social, personal, and economic characteristics to be supplied voluntarily—often eagerly—in order to enjoy the benefits of the economy and the government [40].

There is another side to the coin, however. Since much more information on a person will be stored in the same place, less effort will be necessary to acquire certain "sensitive" data. If insufficient consideration is given to access control and to keeping the price of sensitive information "high enough," the temptation to demand

or to buy this information will increase, since these new systems could be illicitly probed for derogatory information on an individual [59].

Systems with insufficient input checking might be given false and slanderous data about a person which, when printed out on computer output sheets as the result of an inquiry, looks quite "official" and hence is taken as true. "On the horizon in technology is a laser scanning process that would enable a twenty-page dossier to be compiled on each of the 200 million citizens of the United States. Such information could be stored on a single plastic tape reel. Under such conditions it might be cheaper to retain data than to discard it." [9] Clearly, we must decide what information to keep and when to keep it. As Paul Baran points out [4], we face a balance problem. How do we obtain the greatest benefit from computer data banks with the least danger?

LEGAL AND ADMINISTRATIVE SAFEGUARDS

The problem of controlling access to computer files—how to safeguard the processes of inputting to and retrieving from computer data banks—has recently gained more and more attention from concerned citizens. We examine some of this new interest in this section, deferring mention of the technical solutions to the next section.

Bauer has given a brief but sound discussion of policy decisions facing the designers of a computer data bank and has pointed out [6] that we now have the "special but fleeting opportunity . . . to explore the issue of privacy with objectivity and in some leisure. . . . the public's fears of dossier-type police information systems have been thoroughly aroused; left unchecked they may become so strong as to in fact prevent the creation of any publicly supported information systems. The reactions to proposals for a Federal data center are a case in point. Were such blanket prohibitions to be imposed the development of socially useful information-sharing would be enormously impeded. Furthermore, without public trust, information systems could well be fed so much false, misleading or incomplete information as to make them useless. Thus it becomes imperative not only to devise proper safeguards to data privacy, but also to convince the public and agencies which might contribute to a system that these safeguards are indeed being planned, and that they will work."

Fortunately, the Federal Government is aware of the computer privacy problem and has been unreceptive, even hostile, to proposals which do not consider the costs and effectiveness of safeguards necessary to protect privacy in a centralized data bank [56, 57, 68]. Most states, however, lag seriously in awareness of contemporary data processing capabilities and techniques. A few of the more highly computerized areas are, however, trying to approach the idea of regional data banks in a rational manner. At least one state (California) has an intergovernmental board on automatic data processing which has solicited and received comments from concerned members of the technical community on confidentiality and the invasion of privacy.

As Senator Sam J. Ervin, Jr. has pointed out [24], the threat to privacy comes from men, not machines; it comes from the motives of political executives, the ingenuity of managers, and the carelessness of technicians. Too often, he says, an organization may seize upon a device or technique with the best intentions in the world of achieving some laudable goal but in the process may deny the dignity of the individual, the sense of fair play, or the right of the citizen in a free society to the privacy of his thoughts and activities.

"The computer industry, the data processing experts, the programmers, the executives—all need to set their collective minds to work to deal with the impact of their electronic systems on the rights and dignity of individuals.

"While there is still time to cope with the problems, they must give thought to

the contents of professional ethical codes for the computer industry and for those who arrange and operate the computer's processes.

"If self-regulation and self-restraint are not exercised by all concerned with automatic data processing, public concern will soon reach the stage where strict legislative controls will be enacted, government appropriations for research and development will be denied. And the computer will become the villain of our society. It is potentially one of the greatest resources of our civilization, and the tragedy of slowing its development is unthinkable." [24]

Though Senator Ervin gave that speech on 1 May 1967, so far only Chairman Watson of IBM, of all the computer manufacturers, has commented publicly on the subject [60]. The Washington, D.C. Chapter of the ACM has gone on record as opposing the creation of a national data bank until the proposers can show that [58] "such a system is still economically attractive under the legal and technical constraints necessary to protect individual liberties in the American society." (It has been alleged, however, that this vote reflects the views of a minority of that chapter's members and cannot necessarily be taken to represent the view of the chapter.)

We often forget that no "right to privacy," similar to the "right to freedom of speech" or the "right to vote," exists in the Constitution. Thus, the amount of privacy an individual is entitled to and the situations in which that privacy may be violated vary according to the whim of a particular court or legislative body [24, 36, 62]. Prosser, of the University of California School of Law at Berkeley, has compiled an excellent review of this subject [45].

Recently, significant efforts have been made to create a more satisfactory situation. In 1966 John McCarthy suggested a "computer bill of rights." Some of the rights he proposed were these [38]:

—No organization, governmental or private, is allowed to maintain files that cover large numbers of people outside of the general system.

—The rules governing access to the files are definite and well publicized, and the programs that will enforce these rules are open to any interested party, including, for example, the American Civil Liberties Union.

—An individual has the right to read his own file, to challenge certain kinds of entries in his file and to impose certain restrictions on access to his file.

—Every time someone consults an individual's file this event is recorded, together with the authorization for the access.

—If an organization or an individual obtains access to certain information in a file by deceit, this is a crime and a civil wrong. The injured individual may sue for invasion of privacy and be awarded damages.

Additional suggestions have been made concerning legislative methods of safeguarding privacy. In 1967 the United States government proposed a Rights to Privacy Act banning wiretapping and electronic eavesdropping. (In 1968, however, the pendulum swung the other way and the United States Congress passed a "safe streets" and crime-control bill which granted broad authority for wiretapping and eavesdropping, even without a court order, for a limited period of time.)

Even if a statute controlling access to sensitive information in files of the Federal Government were passed, the computer privacy problem would still be a long way from solved. A threat which is possibly even more serious is the misuse of data in the files of private organizations or in the files of state or local governments. Medical records in the files of hospitals, schools, and industrial organizations contain privileged information. When these records are kept in a computer-based system, there must be control over access to them. Some disconcerting examples of what has happened when controls are lax are mentioned in a paper by Baran [4].

California has recently passed into law legislation which (1) recognizes an individual's right of privacy, and (2) recognizes computerized data in state files as "public records." This legislation may well prove to be a landmark in the fight to establish a "right to privacy" and would seem to guarantee the right of an individual to read his own file.

The licensing or "professionalization" of (at least some) computer scientists, programmers, and operators seems to be the most frequent suggestion in the papers on computer privacy which are not written solely for computer scientists. In addition to Ervin (see above), advocates of this measure include Michael [7], Brietson [10], and Ramey [47]. Parker has been the main supporter of the ACM Guidelines for Professional Conduct in Information Processing [41], but Brietson makes the best argument the author has seen for these to date [10]. With such current and potential outside interest in professional conduct of computer people, there has been very little published discussion about these matters. In view of Senator Ervin's unsettling predictions (above), perhaps the computer community should give these problems more attention than it has to date.

This concludes the discussion of legal and administrative safeguards for the protection of sensitive information. We can now turn our attention to the technical solutions that have been proposed.

TECHNICAL METHODS PROPOSED TO DATE

Access Control in Conventional Time-Sharing Systems

Various technical methods for controlling access to the content of computer memories have been suggested. In this discussion these methods are broken up into two categories—those which are necessary for proper operation of a time-sharing system and those which enhance the privacy of data in a shared system.

Methods necessary for a properly operating time-sharing system. First let us consider the controls required in any time-sharing system. A means must be provided to lock out each user from the program and data of all other (unauthorized) users. In addition, a user must not be allowed to interfere with the time-sharing monitor by improper use of input/output commands, halt commands, etc. The latter capability is generally obtained by denying the user certain "privileged" instructions, which may be executed only by "privileged" programs, such as the operating system.

The former is generally provided by memory protection schemes such as relocation and bounds registers [14], segmentation [12, 31], paging [51], and memory keys which allow limited (e.g. read-only) access [32].

All these access control methods protect contiguous portions of (real or virtual) computer memory from alteration by an errant program. They do not, however, provide protection of a user file from unauthorized access. Toward this end, software schemes have augmented the hardware schemes described above.

Methods which enhance data privacy. With respect to the methods which enhance the privacy of data in a shared system, Paul Baran observed in 1966 [5] that "It is a very poorly studied problem . . . There is practically nothing to be found in the computer literature on the subject." Since then, awareness has grown, largely as a result of Congressional interest [56, 57]. An entire session of the AFIPS 1967 Spring Joint Computer Conference was devoted to this issue. But only very recently has there been developed a working system with more than password protection at the file level [29].

In nearly all systems to date, a user's password (see Figure 1) will get him into his file directory and into any file referenced in that directory. The most elaborate scheme so far is that of Daley and Neumann [16], which features directories nested to any level used in conjunction with passwords. Each file has access control information associated with itself. Unless one has the "key" to a file, one cannot get at the information in that file. Password schemes permit a small finite number of specific types of access to files, although Daley and Neumann [16] effectively provide more flexible control via a type which allows a user-written program to decide whether each requested access to a file is allowed.

Limitations of these methods. The meth-

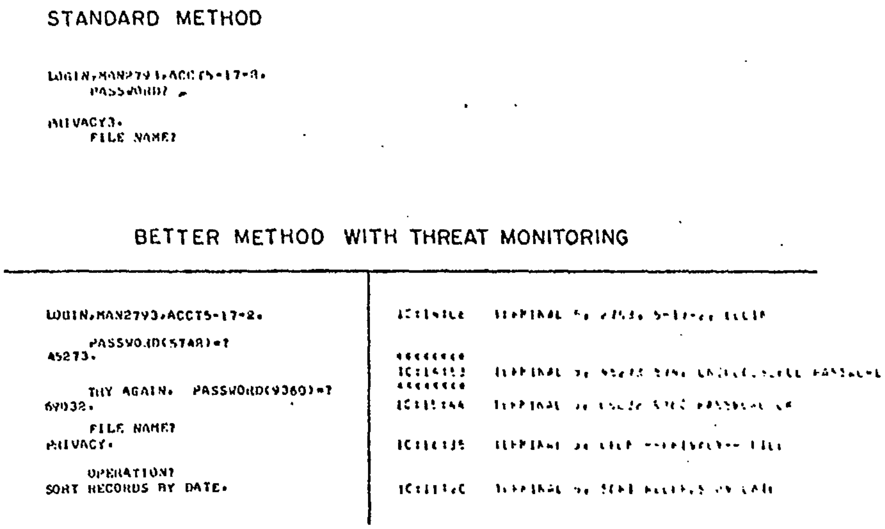


Fig. 1. Password use

ods above necessary for properly operating a time-sharing system perform their task acceptably—they guarantee system integrity. However, the password methods fall short of providing adequate software protection for sensitive files. Password schemes can be compromised by wiretapping or electromagnetic pickup, to say nothing of examining a console typewriter ribbon. Moreover, in some systems the work factor, or cost, associated with trying different passwords until the right one is found is so small that it is worthwhile for an interested but unauthorized user to do just that. Centralized systems tend to have relatively low work factors, since breaking a code in a centralized system generally allows access to more information than in a decentralized system. Some methods used to raise the work factor back to at least the level of a decentralized system are given below.

There is an even more serious problem with password systems. In most current systems, information is protected at the file level only—it has been tacitly assumed that all data within a file was of the same sensitivity. The real world does not conform to these assumptions. Information from various sources is constantly coming into common data pools, where it can be used by all persons with access to that pool. The problem of what to do when certain information in a file should be available to some but not all legal users of the file is not well studied. In the Multics system [12], for example, it is currently the case that if a user has a file which in part contains sensitive data, he just cannot merge *all* his data with that of his colleagues. He must separate the sensitive data and save that in a separate file; the common pool of data does not contain this sensitive and possibly highly valuable data. Moreover, he and those he allows to access this sensitive data must, if they also want to make use of the nonsensitive data, create a distinct merged file, thus duplicating information kept in the system; if some of this duplicated data must later be changed, it must be changed in all files, instead of only one (see Figure 2). If there was a method for placing data with varying degrees of sensitivity into common files such that suitable access control over each piece of data was guaranteed, all the data could be aggregated and processed much more easily. Indeed, many social scientists are in favor of a national data bank for this very reason [8, 20]. On the other hand, precisely because the problem has not been solved

satisfactorily, lawyers [22, 48] scientists [5, 11, 19, 28, 54], urban planners [65], and the general public [53, 55, 63] have become concerned about such a system.

In a recent thesis, Hsiao [29] has suggested and implemented files which contain "authority items"; these authority items control access to records in files. Other proposals which treat access control as a function of the user rather than the data have been advanced by Evans and LeClerc [66] and by Bingham [64]. Hsiao's scheme, however, is the first *working* system which controls access at a level lower than the file level. The implementation depends on a multilist [46] file structure, but the concept of an authority item associated with each user is independent of the structure of the file. The accessibility of a record depends on whether the file owner has allowed access to the requester. This information is carried in the authority item. Capabilities [18] (such as read only, read and write, write only) appear to reside with the file rather than with each record.

A problem with Hsiao's scheme is the duplication in *each pertinent* authority item of entries for protected fields of *one* file. If there are J users of the system and each has K private fields in each of L files, and if each user has access to the files of S other users, then $S \times K \times L$ entries must be made in *each* authority item for user protection. Since there are J users, $T = J \times S \times K \times L$ entries must be maintained in the authority items by the system. For the not unlikely case $J = 200$, $K = 3$, $L = 2$, $S = 10$, we calculate $T = 12{,}000$. Depending on the amount of storage used per entry, this price in storage and maintenance may prove too much to pay in many instances. As S approaches $J - 1$, not only does this price become higher but the system also becomes inefficient (since it maintains lists of *authorized* rather than *unauthorized* file users). Of course, if $S = J - 1$, the entire protection system is unnecessary.

Some other methods for access control have been proposed. Graham [27] has suggested a technique involving concentric "rings" of protection which may prove a reasonable way to provide flexible but controlled access by a number of different users to shared data and procedures. Dennis and Van Horn [18] have proposed that higher-level programs grant access privileges to lower-level programs by passing them "capability lists."

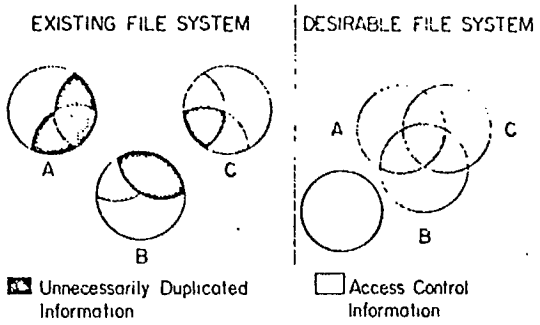


FIG. 2. Use of computer storage in file systems

Graham's scheme has several disadvantages. It assumes a computer with demand hardware segmentation; since, in the opinion of the author, no large computer systems (of the type that would be necessary for a public utility) with these hardware facilities are as yet serving a large user community in an acceptable manner, this assumption may be premature, particularly in light of the alternatives, such as monoprogramming systems which use extended core storage bulk memories [30, 37]. The Graham scheme effectively rules out the use of one-level memories such as associative memories [25], Lesser memories [35], etc., given the current hardware state-of-the-art. If the data bank has many different data fields with many different levels of access, the swap times necessary to access each datum in its own (two-word or so) segment will rapidly become prohibitive using today's technology. In addition, the Graham scheme imposes a hierarchy on all information in the data base; this is not desirable in every instance. The scheme of Dennis and Van Horn suffers from all the drawbacks of the Graham scheme except the last. Com-

TABLE I. SOME THREATS TO INFORMATION PRIVACY (Extracted from [44])

Accidental
User error
System error
Deliberate, passive
Electromagnetic pick-up
Wiretapping
Deliberate, active
Browsing
Masquerading as another user
"Between lines" entry while user is inactive but on channel
"Piggy back" entry by interception and transmitting an "error" message to the user
Core dumping to get residual information

pensating for this relative simplicity in the control structure, however, is the fact that a very large number of their meta-instructions must be executed for each attempt to access data which is not in a file open to every user.

Some Proposed Safeguards for the Privacy of Information in Files

We now discuss countermeasures that have been proposed to more adequately insure against unauthorized access to information in files. Petersen and Turn have published an excellent paper [44] on the threats to information privacy, and much of the material of this section has been drawn from that paper.

The most important threats to information privacy are shown in Table I. We can counter these threats by a number of techniques and procedures. Petersen and Turn have organized the various countermeasures into several classes: access management, privacy transformations, threat monitoring, and processing restrictions. They have one other class, integrity management (of hardware, software, and personnel), which is not discussed here.

Access management. These techniques attempt to prevent unauthorized users from gaining access to files. Historically, passwords have been almost synonymous with access management. Passwords alone, however, are not enough, as shown above. The real issue in access management is *authentication* of a user's identification. Peters [43] has suggested using one-time passwords: lists of randomly selected passwords would be stored in the computer and maintained at the terminal or kept by the user. "After signing in, the user takes the next work (sic) on the list, transmits it to the processor and then crosses it off. The processor compares the received password with the next word in its own list and permits access only when the two agree. Such password lists could be stored in the terminal on punched paper tape, generated internally by special circuits, or printed on a strip of paper. The latter could be kept in a secure housing with only a single password visible. A special key lock would be used to advance the list." [44] Another method, based on random-number generation, has been suggested by Baran [3].

A novel idea based on the same principle—the high work factor [3] associated with breaking encoded messages appearing as pseudorandom or random number strings [52]—has been suggested by Les Earnest [23]. He proposes that the user log in and identify himself, whereupon the computer supplies a pseudorandom number to the user (see Figure 1). The user performs some (simple) mental transformation T on the number and sends the result of that transformation to the computer. The computer then performs the (presumably) same transformation, using an algorithm previously stored in (effective) execute-only memory at file creation time. In this way, while the user has performed T on x to yield $y = T(x)$, any "enemy" tapping a line, even if the information is sent in the clear, sees only x and y. Even simple T's, e.g.

$$T(x) = \left[\left(\sum_{i \text{ odd}} \text{digit } i \text{ of } x\right)^{3/2}\right] + (\text{hour of the day}),$$

are almost impossible to figure out, and the "cost per unit dirt" [2] is, hopefully, much too high for the enemy. Petersen and Turn point out that one-time passwords are not adequate against more sophisticated "between lines" entries by

infiltrators who attach a terminal to the legitimate user's line. "Here the infiltrator can use his terminal to enter the system between communications from the legitimate user." [44] As a solution, they suggest one-time passwords applied to messages (as opposed to sessions), implemented by hardware in the terminal and possibly in the central processor. This solution may, however, be too costly for most applications. Also, placing access control at the datum level, rather than at the file level, would eliminate many (though not all) problems associated with this type of infiltration.

Babcock [1] mentions a "dial-up and call-back" system for very sensitive files. When a sensitive file is opened by the program of a user who is connected to the computer via telephone line A, a message is sent to the user asking him to telephone the password of that file to the operator over a different telephone line B. The legal user can alter the password at will by informing the data center.

Privacy transformations. Privacy transformations are reversible encodings of data used to conceal information. They are useful for protecting against wiretapping, monitoring of electromagnetic radiation from terminals, "piggy-back" infiltration (see Table II), and unauthorized access to data in removable files. Substitution (of one character string for another), transposition (rearrangement of the ordering of characters in a message), and addition (algebraically combining message characters with "key" characters to form encoded messages) are three major types of privacy transformations, which can be (and are) combined to increase the work factor necessary to break a code. This work factor depends (among others) on the following criteria [52]:

1. Length of the key. Keys require storage space, must be protected, have to be communicated to remote locations and entered into the system, and may even require memorization. Though generally a short key length seems desirable, better protection can be obtained by using a key as long as the message itself.

2. Size of the key space. The number of different privacy transformations available should be as large as possible to discourage trial-and-error approaches, as well as to permit the assignment of unique keys to large numbers of users and changing of keys at frequent intervals.

3. Complexity. The cost of implementation of the privacy system is affected by requiring more hardware or processing time, but the work factor may also be improved.

4. Error sensitivity. The effect of transmission errors or processor malfunctioning may make decoding impossible.

Other criteria are, of course, the cost of implementation and the processing time requirements which depend, in part, on whether the communication channel or the files of the system are involved.

More detailed information on uses of privacy transformations is given in Petersen and Turn [44]. A good unclassified discussion of encrypting and cryptanalysis methods, with particular attention paid to "distributed" communication networks (many terminals, many message switching centers, etc.) has been written by Baran [3]. He also has suggested [2] that we should always make use of minimal privacy transformations in the storage and transmission of sensitive data.

Privacy transformations can be performed by appropriate software in terminals and central processors. When desirable, hardware can be used instead. One current system, for example, uses basically a transposition method and is handled with preset plastic scrambler wheels; changes of these wheels are accomplished by time coordination [39].

Threat Monitoring. Petersen and Turn give a good description of threat monitoring [44]: "Threat monitoring concerns detection of attempted or actual penetrations of the system or files either to provide a real-time response (e.g. invoking job cancellation, or starting tracing procedures) or to permit *post facto* analysis. Threat monitoring (see Figure 1) may include the recording of all rejected attempts to enter

the system or specific files, use of illegal access procedures, unusual activity involving a certain file, attempts to write into protected files, attempts to perform restricted operations such as copying files, excessively long periods of use, etc. Periodic reports to users on file activity may reveal possible misuse or tampering, and prompt stepped-up auditing along with a possible real-time response."

Threat monitoring also will help improve the efficiency of the system by reporting widespread use of particular system facilities. These system facilities can be

TABLE II. SUMMARY OF COUNTERMEASURES TO THREATS TO INFORMATION PRIVACY (extracted from [44])

Threat \ Countermeasure	Privacy Transformations	Threat Monitoring (audits, logs)
Accidental:		
User error	No protection if depend on password; otherwise good protection	Identifies the "accident prone"; provides post facto knowledge of possible loss
System error	Good protection in case of communication system switching errors	May help in diagnosis or provide post facto knowledge
Deliberate, passive:		
Electromagnetic pick-up	Reduces susceptibility; work factor determines the amount of protection	No protection
Wiretapping	Reduces susceptibility; work factor determines the amount of protection	No protection
Deliberate, active:		
"Browsing"	Good protection	Identifies unsuccessful attempts; may provide post facto knowledge or operate real-time alarms
"Masquerading"	No protection if depends on password; otherwise, sufficient	Identifies unsuccessful attempts; may provide post facto knowledge or operate real-time alarms
"Between lines" entry	Good protection if privacy transformations changed in less time than required by work factor	Post facto analysis of activity may provide knowledge of possible loss
"Piggy back" entry	Good protection if privacy transformations changed in less time than required by work factor	Post facto analysis of activity may provide knowledge of possible loss
Entry by system personnel	Work factor, unless depend on password and masquerading is successful	Post facto analysis of activity may provide knowledge of possible loss
Entry via "trap doors"	Work factor, unless access to keys obtained	Possible alarms, post facto analysis
Core dumping to get residual information	No protection unless encoded processing feasible	Possible alarms, post facto analysis
Physical acquisition of removable files	Work factor, unless access to keys obtained	Post facto knowledge form (sic) audit of personnel movements

"tuned," or, if need be, the facilities can be altered to eliminate bottlenecks. If some security restriction is unduly interfering with system operation, threat monitoring should help pinpoint the offending restriction.

Processing restrictions. In addition to the normal memory protection features mentioned in the first part of this section, some processing restrictions may be desirable. Suggestions have included the mounting of removable files on drives with disabled circuits which must be authenticated before access [44], erasure of core

TABLE II. *Continued*

Threat \ Countermeasure	Access Control (password, authentication, authorization)	Processing Restrictions (storage, protected privileged operations)
Accidental: User error	Good protection, unless the error produces correct password	Reduce susceptibility
System error	Good protection, unless bypassed due to error	Reduce susceptibility
Deliberate, passive: Electromagnetic pick-up	No protection	No protection
Wiretapping	No protection	No protection
Deliberate, active: "Browsing"	Good protection (may make masquerading necessary)	Reduces ease to obtain desired information
"Masquerading"	Must know authenticating passwords (work factor to obtain these)	Reduces ease to obtain desired information
"Between lines" entry	No protection unless used for every message	Limits the infiltrator to the same potential as the user whose line he shares
"Piggy back" entry	No protection but reverse (processor-to-user) authentication may help	Limits the infiltrator to the same potential as the user whose line he shares
Entry by system personnel	May have to masquerade	Reduces ease of obtaining desired information
Entry via "trap doors"	No protection	Probably no protection
Core dumping to get residual information	No protection	Erase private core areas at swapping time
Physical acquisition of removable files	Not applicable	Not applicable

memories after swapping a program and its data out to an auxiliary storage device, and built-in hardware codes which peripheral devices would transmit to other system components when necessary. Software which limits access rights by terminal is already part of several systems [69].

There is a real question as to what price one is willing to pay for a given amount of privacy [61]. In some instances, one might desire a whole processor to implement the entire file control and privacy system [44]. Most users, however, will probably settle for less privacy at less cost. This has been the experience so far of Allen-Babcock Corporation—they have not implemented their "dial-up and call-back" privacy technique, since none of their customers has demanded it.

Petersen and Turn have summarized their countermeasures to threats against information integrity, and the major part of the table they present is reproduced in Table II.

PROMISING RESEARCH PROBLEMS

In this section we briefly outline some technical problems which offer promising avenues for research in the future. We raise relevant questions, but no answers are proposed in this paper.

For reasons mentioned in the section on the limitations of proposed protection methods, the methods of protection which effectively pass privileges from one program to another are unsatisfactory. We also saw there that protecting data by associating controls with the data at the file level only is not sufficient. What is needed is some means of controlling access to each individual datum. Such a means should (1) be efficient, and (2) not unduly penalize the user who only wants a small part of his file protected. The mechanism may reside in program, data, indexes into an inverted file, authority items [29], or elsewhere.

Several types of controls have been proposed to insure privacy: threat monitoring, privacy transformations, access management, etc. Some hardware countermeasures, such as physical keys which record the key number on a file or output device, have also been suggested. Unfortunately, no systems, hardware or software, simulated or actual, have been built which enable us to evaluate the various costs of processing time, storage space, etc., of these methods. There is almost a complete absence of implementation of nearly all the proposed techniques. Consider, for example, just one of these techniques, privacy transformations. Petersen and Turn [44] discuss the further work that is needed: "Special attention must be devoted to establishing the economic and operational practicality of privacy transformations: determining applicable classes of transformations and establishing their work factors; designing economical devices for encoding and decoding; considering the effects of query langauge structure on work factors of privacy transformation; and determining their effects on processing time and storage requirements."

The implementation of a (real or simulated) system which uses many countermeasure techniques would be a very desirable undertaking. It would enable us to evaluate the effectiveness and the costs of each technique. A suitably designed system would at the same time allow us to vary the structure of a file. Since the structure of a file may affect quite strongly the access control method used, a number of interesting experiments could be performed. For example, one might consider physically separating the more sensitive data in a hierarchical tree-structured file from the less sensitive data. The more sensitive data could be stored in a memory which was logically at a low level and physically removed from higher-level data. This solution would not be feasible in certain types of associative memories, since the control would require all data to be at the same level.

As another example, the existence of indexes into a tree-structured file (i.e. the use of an inverted file) might strongly alter the operating characteristics of the

access control mechanism by allowing control information to reside in the indexes rather than (say) with the data itself. Further investigation of this relationship is also warranted.

SUMMARY

It is hoped that this paper may help increase awareness of the computer privacy problem and the need for further investigation. Paul Baran puts it well [2]:

"What a wonderful opportunity awaits the computer engineer to exercise a new form of social responsibility. The advent of the new computer-communications technology need not be feared with trepidation as we approach 1984. Rather, we have in our power a force which, if properly tamed, can aid, not hinder, raising our personal right of privacy.

"If we fail to exercise this unsought power that we computer engineers alone hold, the word 'people' may become less a description of individual human beings living in an open society and more a mere collective noun.

"It may seem a paradox, but an open society dictates a right-to-privacy among its members, and we will have thrust upon us much of the responsibility of preserving this right."

ACKNOWLEDGMENTS

The author wishes to thank Professor William F. Miller and Mr. John V. Levy for their encouragement during the preparation of this paper.

BIBLIOGRAPHY

1. Babcock, J. D. A brief description of privacy measures in the RUSH time-sharing system. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D. C., pp. 301–302.

   A brief summary of the file security procedures in RUSH. This article contains some good but short discussion of possible threats and countermeasures.

2. Baran, P. Communications, computers and people. AFIPS 1965 Fall Joint Comput. Conf. Vol. 27, Pt. 2, Thompson Book Co., Washington, D. C., pp. 45–49.

   A well-thought-out general discussion of the privacy problem which overlaps somewhat with Baran's testimony before the Gallagher subcommittee (see [56]). Some specific proposals are presented to deal with the problem.

3. Baran, P. On distributed communications: IX. Security, secrecy and tamper-free considerations. Doc. RM-3765-PR, Rand Corp., Santa Monica, Calif., Aug. 1964.

   A consideration of the security aspects of a distributed communication system, written from the viewpoint that we should fully anticipate the existence of spies within our ostensibly secure communications secrecy protection structure; "Hence, our primary interest should be in raising the 'price' of espied information to a level which becomes excessive." The proposed system combines end-to-end and link-by-link cryptography, automatic error detection and repeat transmission, path changing, and use of a scheme requiring complete and correct reception of *all* previous traffic in a conversation in order to decrypt subsequent message blocks. It assumes enemy infiltration and takes these countermeasures: key bases split over N (> 1) individuals; filtering tests; key change for each conversation; heavy system use for unclassified traffic. Contents: I. Introduction; II. The Paradox of Secrecy about Secrecy; III. Some Fundamentals of Cryptography; IV. Implications for the Distributed Network System; V. A "Devil's Advocate" Examination.

   This paper gives a clear, well-written discussion of an often "touchy" subject. Relevant points are brought out by good diagrams. It is one of the clearest expositions of real-life problems and solutions to be found in the open literature.

4. Baran, P. Remarks on the question of privacy raised by the automation of mental health records. Doc. P-3523, Rand Corp., Santa Monica, Calif., Apr. 1967.

   Remarks invited for presentation before the American Orthopsychiatric Association Workshop, "The Invasion of Privacy," held in Washington, D. C., 21–23 March 1967. This speech of Baran presents to an intelligent group of computer laymen a view of computer privacy invasion which heretofore has been available only to people in the computer field. Some tales of medical record leaks are recalled. The famous tale of the MIT freshman who programmed the computer to dial simultaneously every telephone extension in the school is retold; thus the importance of "people-proof" systems is graphically illustrated.

   It is a very good paper which can be used to alert intelligent people to the implications of the computer age for privacy.

5. Baran, P. Statement in [56], pp. 119–135.

6. Bauer, K. G. Progress report to U. S. Public Health Service on contract PH 110-234. Joint

Center for Urban Studies of MIT and Harvard, Cambridge, Mass., Jan. 1968. (Mimeographed)

The report contains a nine-page section on the privacy issue as it relates to a proposed health information system for the Boston area. "... Right now our project has a unique opportunity to propose safeguards to privacy in the design of an information system at a time when the crucial operational decisions have not yet been made...." The section discusses present safeguards to record disclosure. Currently, privacy is not really insured, and only the excessive cost of getting sensitive information (because of the unwieldiness of current noncomputerized systems) prevents almost all unauthorized access. "... With proper safeguards computerization makes such information far easier to guard..."—why this is the case is explained. A broad framework of new safeguards, combining legal, technological, and administrative measures is being urged, and these are gone into very briefly, with references to a few papers. The committee hopes during the coming months to define levels of security and to suggest specific access rules and rights of patients that should be kept in mind.

7. Berkeley, E. C. Individual privacy and central computerized files. *Comput. Automat. 15*,10 (Oct. 1966), 7.

This article discusses a privacy bill of rights initially suggested by Professor John McCarthy in [38].

8. Bowman, R. T. Statement in [56].

9. Brigham, R. C. Computers and privacy—implications of a management tool. Doc. SP-2953/001/00, System Development Corp., Santa Monica, Calif., 14 Mar. 1968.

10. Brigham, R. C. Some thoughts on the social implications of computers and privacy. Doc. SP-2953, System Development Corp., Santa Monica, Calif., 25 Sept. 1967.

This is a reprint of a talk presented to the American Society for Industrial Security as part of a panel, "Problems in the Age of the Computer," 13th annual seminar, 12–14 September 1967, Los Angeles, California. Briefly discussed are (1) the computer as an innovation and tool, along with some of the anxieties it creates, (2) a framework for an inquiry into the problem, (3) responsibilities of organizations and the establishment, (4) socialization—the preparation of new members for entry into society, (5) some examples reflecting issues, and (6) possible remedies. In eleven short pages a quite readable discussion, understandable to the lay person, is given. The framework suggested for investigation seems quite reasonable, and represents one of the few attempts to define the general problem before rushing off to tackle it. This structure considers information from the standpoint of (1) acquisition; (2) access; (3) dissemination; (4) retention; (5) revision, including updating, rejoinder and redress; (6) destruction; and (7) time cycles. Brief examples are given for acquisition and protection. A good case (and a brief one) for the existence of professional ethics codes is made, much better than the discussion in [41] by Parker. Five guidelines for public policy makers are suggested: (1) specifications of benefits; (2) catalogue of potential risks; (3) directory of preventive safeguards and controls; (4) inventory of antidotes and countermeasures; (5) index of penalties and sanctions.

A very good paper for the layman and interested computer scientist.

11. Caldwell, L. K. (Ed.) *Science, Technology, and Public Policy—A Selected and Annotated Bibliography (Volume 1)*. Dep. of Government, Indiana U., Bloomington, Ind., 1968, pp. 207–210.

Pages 207–210 comprise Section 6.4, "Privacy," and contain an annotated bibliography of 13 entries. [40] and [22] are included, and [62] is based on two other entries in the bibliography. The others deal with privacy as an aspect of human dignity, lie detectors, wiretapping, concepts of consent and confidentiality, and eavesdropping. The entire bibliography should be useful to students of sociology. Its sections are:

1. Bibliographies and Research Tools
2. Philosophy of Science
3. History of Science and Technology
4. Nature and Impact of Science and Technology
5. Science, Politics, and Government
6. Science, Technology, and the Law
7. Science, Education, and the Universities
8. Scientific and Technical Personnel
9. Scientific Organizations and Institutions
10. Organization and Management of Research and Development
11. Science, the Humanities, and Religion
12. Science and Society

12. Corbato, F. J., and Vyssotsky, V. A. Introduction and overview of the Multics system. Proc. AFIPS 1965 Fall Joint Comput. Conf., Vol. 27, Pt. 1, Spartan Books, New York, pp. 185–196.

13. Computer Research Corp. Time-sharing system scorecard, No. 5. Computer Research Corp., Newton, Mass., 1967.

14. Control Data Corp. Control Data 6100/6600 computer systems reference manual. Pub. No. 60100000, Control Data Corp., St. Paul, Minn., 1966.

15. Crisman, P. A. (Ed.). *The Compatible Time-Sharing System—A Programmer's Guide* (Second ed.). MIT Press, Cambridge, Mass., 1965.

16. Daley, R. C., and Neumann, P. G. A general-purpose file system for secondary storage. Proc. AFIPS 1965 Fall Joint Comput. Conf., Vol. 27, Pt.1, Spartan Books, New York, pp. 213–229.

This system places access control on the branches of a tree-structured file directory. Five modes of control are allowed—trap, read, execute, write, and append. The paper contains some of the best thinking yet about a practical, general solution to lower-level access control. One of the "Multics papers," this is must reading for data base system designers.

17. Davies, L. E. Computer plan for personal

"dossiers" in Santa Clara stirs fears of invasion of privacy. *The New York Times*, 1 Aug. 1966, p. 27.

18. Dennis, J. B., and Van Horn, E. C. Programming semantics for multiprogrammed computations. *Comm. ACM 9*,3 (Mar. 1966), 143–155.

A number of meta-instructions are defined which relate to programming operations in multiprogrammed systems. These are related to parallel programming, protection of separate computations, sharing of files, and memory. Some very good and long-neglected ideas are set forth here. Capabilities of a computation are related to segments. In practice, capabilities should be related to some smaller basic units, e.g. nodes of a tree.

19. Deutsch, L. P. Snooping by computer (letter to the editor). *San Francisco Chronicle*, 19 July 1968.

A computer scientist experienced in time-sharing systems warns against misuse of computers. In particular, he laments the lack of adequate protection in the California Department of Social Welfare data bank.

20. Dunn, E. S., Jr. Statement in [56], pp. 92–95.

21. Dunn, E. S., Jr. The idea of a national data center and the issue of personal privacy. *Amer. Statis. 21* (Feb. 1967), 21–27.

An attempt by the author of the Bureau of the Budget report which recommended the establishment of a national data center to correct "certain obvious misinterpretations and set forth more explicitly some views on the very important issue of personal privacy." He maintains that we can immediately begin to save much "harmless" data in a "statistical" data bank and that we have 10 or 15 years to figure out how to protect privacy. The trade-offs for and against some sort of national data bank are more clearly delineated than in the original report.

22. Duke University School of Law. Privacy. *Law and Contemporary Problems 31*, 2 (Spring 1966), 251–435.

This is an entire issue of *Law and Contemporary Problems* devoted to privacy. Its contents are: Clark C. Havighurst, "Foreword"; William M. Beany, "The Right to Privacy and American Law"; Milton R. Konvitz, "Privacy and the Law: A Philosophical Prelude"; Edward Shils, "Privacy: Its Constitution and Vicissitudes"; Sidney M. Jourard, "Some Psychological Aspects of Privacy"; Glenn Negley, "Philosophical Views on the Value of Privacy"; Harry Kalven, Jr., "Privacy in Tort Law—Were Warren and Brandeis Wrong?"; Kenneth L. Karst, "'The Files': Legal Controls Over the Accuracy and Accessibility of Stored Personal Data"; Joel F. Handler and Margaret K. Rosenheim, "Public Assistance and Juvenile Justice"; William A. Creech, "The Privacy of Government Employees."

The issue contains nothing on computers except in the Karst paper, which has about four pages on the effect of automation. The possible solutions to this aspect of the privacy problem are dealt with in superficial detail, but relevant references are given for the reader interested in a more advanced technical discussion.

23. Earnest, L. Private communication.

24. Ervin, S. J. The computer—individual privacy. *Vital Speeches of the Day 33*, 14 (1 May 1967), 421–426.

Senator Ervin discusses the impact of the computer on national life in a speech to the American Management Association. He thinks that in order to avoid strict legislative controls and the denial of government research and development funds, the industry must devise safeguards against improper data access, illegal tapping, and purloined data in shared systems. He likes the idea of an industry ethical code.

25. Feldman, J. A. Aspects of associative processing. Tech. Note 1965-13. Lincoln Laboratory, MIT, Cambridge, Mass., 1965.

26. Gallati, R. R. J. The New York State identification and intelligence system. In [56], pp. 159–168.

27. Graham, R. M. Protection in an information processing utility. *Comm. ACM 11*, 5 (May 1968), 365–369.

A good five-page paper on the topic. A solution to the file access problem is given which involves rings or spheres of protection for both data and programs (in particular, for segments, as at Project MAC). The main drawbacks are (1) the method is tied to segments, which in practice are fairly large blocks of memory; protection of a smaller area wastes the rest of the segment; and (2) parallel processes or processors may render parameters or data invalid if proper safeguards are not taken. If these problems are solved, this method provides flexible but controlled access by a number of different users to shared data and procedures.

28. Harrison, A. The problem of privacy in the computer age: an annotated bibliography. Doc. RM-5495-PR/RC, Rand Corp., Santa Monica, Calif., Dec. 1967.

This is a must document. This 300-entry bibliography is well-annotated and indexed by author as well as by each of the following categories: cashless-checkless society, time-sharing, data banks, media, social scientists' views, bill of rights, electronic eavesdropping and wiretapping, computer utilities, Congressional view of privacy, legal views, system security, technologists' views.

29. Hsiao, D. K. *A File System for a Problem Solving Facility*. Ph.D. Diss. in Electrical Engineering, U. of Pennsylvania, Philadelphia, Pa., 1968.

An important new concept is introduced and implemented on the file system at Penn. This concept, that of the authority item, allows control within files over data access. Each field in a file can be protected from unauthorized access. Data records need not be reprocessed if a change in a record's protection status or in a user's level of accessibility occurs. The capability to read only, write only,

etc., goes with an authority item and not with a record. Protected records are completely nonexistent as far as the unauthorized user is concerned. The system as currently implemented is dependent on the file structure (multilists). However, the idea of authority items is not and is an important new concept. This thesis should be examined by those who have the responsibility for access control in their own file systems. It appears to be the first working system with protection below the file level.

30. HUMPHREY, T. A. Large core storage utilization in theory and in practice. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 719–727.

31. IBM System/360 Model 67 functional characteristics. Form A27-2719-0, IBM Corp., Kingston, N. Y., 1967.

32. IBM System/360 principles of operation. Form A22-6821-2, IBM Corp., Poughkeepsie, N. Y., 1966.

33. JANSSEN, R. F. Administration studies plan to generalize data, hopes to avoid "police state" image. *Wall Street J.*, 11 Nov. 1966, p. 6.

34. KAYSEN, C. Data banks and dossiers. *The Public Interest* (Spring 1967); also in [57], p. 265.

The case "for" a national data bank, in the light of the mauling this proposal got before the Gallagher subcommittee.

35. LESSER, V. R. A multi-level computer organization designed to separate data-accessing from the computation. Tech. Rep. CS90, Comput. Sci. Dep., Stanford U., Stanford, Calif., 11 Mar. 1968.

36. LICKSON, C. P. The right of privacy in the computer age. *IEEE Comput. Group News 2*, 1 (Jan. 1968), 13–17.

A nontechnical five-page paper which defines privacy, examines some historical court cases dealing with it, and tries to pinpoint current legislative trends in this area. "... Legislation and court decisions can catch up to the state of the art." A good general overview from a nontechnical standpoint, the article is well-referenced.

37. MACDOUGALL, M. H. Simulation of an ECS-based operating system. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 735–741.

38. MCCARTHY, J. Information. *Sci. Amer. 215*, 3 (Sept. 1966), 64–73.

McCarthy, in a very good survey article on computation, proposes a computer bill of rights which would help to guarantee privacy in computer-based data files.

39. MCLAUGHLIN, F. X. Private communication.

40. MICHAEL, D. N. Speculations on the relation of the computer to individual freedom and the right to privacy. *George Washington Law Rev. 33* (1964–65), 270–286.

Between now and 1984, business and government will use extraordinary advances in computer technology to file and collate "personal" facts about private citizens and even to telemeter the populace. What are the implications for traditional ideas of freedom and privacy? Will such progress be met with constitutional objections or with public acquiescence?—Author's Abstract

This well-written nontechnical paper makes some valid and oft-overlooked points. It outlines factors which, in the past, have made privacy invasion difficult: (1) data available but uncollected and uncollated; (2) data not recorded with precision and variety necessary to gain new or deeper insight into the private person; (3) difficulty of keeping track of a particular person in a large and highly mobile population; (4) difficulty of access to already filed data about the private person; (5) difficulty of detecting and interpreting potentially self-revealing private information within available data.

Points for a central data bank are validly and tellingly made, and the point is made that now, as in the past, people may give up some freedom to protect or enhance another freedom. Ways in which corruptible programmers may become privy quite legally to privileged information are discussed. A short and worthwhile paper.

41. PARKER, D. B. Rules of ethics in information processing. *Comm. ACM 11*, 3 (Mar. 1968), 198–201.

42. PARKER, R. W. The SABRE system. *Datamation 11*, 9 (Sept. 1965), 49–52.

43. PETERS, B. Security considerations in a multiprogrammed computer system. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 283–286.

A specific list of desirable and necessary security safeguards for file systems is given. Hardware, software, and administrative safeguards are discussed.

44. PETERSEN, H. E., AND TURN, R. System implications of information privacy. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 291–300. (Also available as Doc. P-3504, Rand Corp., Santa Monica, Calif., Apr. 1967.)

"Various questions of providing information privacy for remotely accessible on-line, time-shared information systems are explored.... A range of protective countermeasures is discussed, and their choice and implication considered. It appears possible to counter a given level of threat without unreasonable expenditures of resources. The protective techniques discussed ... include: shielding to reduce electromagnetic emanations; use of once-only passwords for access control; application of privacy transformations to conceal information in user-processor communications and in data files; recording of attempted penetrations; and systematic verification of the hardware and software integrity."—Authors' abstract

This is must reading. It contains a detailed and well-written discussion of threats to file security and countermeasures against these

threats. In particular, problems at the processor, the files, the terminals, and the communication lines are discussed. A good bibliography is given.

45. Prosser, W. L. Privacy. *California Law Rev. 48*,3 (Aug. 1960), 383–423.

A review of court cases dealing with a "right to privacy." The review appears to be comprehensive (to this layman at law). The author, then Dean of the University of California Law School at Berkeley, contends that four distinct kinds of privacy invasion cases can be described: (1) intrusion upon seclusion or solitude, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places the plaintiff in a false light in the public eye; (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. The article is well-written and interesting. As a final fillip, I can not conclude without praising the author for making me aware of "a possible nomination for the all-time prize law review title, in the note 'Crimination of Peeping Toms and Other Men of Vision,' *Ark. Law Rev. 6*(1951), 388."

46. Prywes, N. S. A storage retrieval system for real-time problem solving. Rep. No. 66-05, U. of Pennsylvania Moore School of Electrical Engineering, Philadelphia, Pa., 1966.

47. Ramey, J. W. Computer information sharing—threat to individual freedom. Proc. of the Amer. Documentation Institute, 1967, pp. 273–277.

This paper discusses, for a lay audience, why centralized data banks threaten privacy. It proposes licensing of computer professionals, much as CPA's are licensed now. It also proposes legislation to allow an individual to inspect his entire dossier, delete inaccuracies via court order, and prohibit transfer of information identifiable with himself to a linked data bank without his express consent.

48. Reich, C. A. Statement in [56].

49. Schwartz, J. I. The SDC time-sharing system. *Datamation 10*,11 (Nov. 1964), 28–31.

50. Schwartz, J. I. The SDC time-sharing system. *Datamation 10*,12 (Dec. 1964), 51–55.

51. Scientific Data Systems. SDS 940 computer reference manual. Pub. No. 90 06 40A, Scientific Data Systems, Santa Monica, Calif., Aug. 1966.

52. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J. 28*, 4 (Oct. 1949), 656–715.

A mathematical theory of secrecy systems is developed and presented in a most readable form. First, basic mathematical structure of secrecy systems is dealt with. Examples of various types of ciphers are given. Measures of "how secret" a system is are introduced, and it is shown that "perfect" secrecy is possible but requires, if the number of messages is finite, the same number of possible keys. A measure of "noise" in a message is given and strongly ideal systems where this cannot be decreased by the cryptanalyst are discussed. Finally, an analysis of the basic weaknesses of secrecy systems is made. This leads to methods for constructing systems which require a large amount of work to solve. Finally, a certain incompatibility among the various desirable qualities of secrecy systems is discussed. An excellent paper, and doubly so for the nonfaintheartedin mathematics (particularly probability and modern algebra).

53. Social workers balk at computers. *San Francisco Chronicle*, 16 July 1968, p. 2.

This newspaper article describes how over 20 state social workers picketed the state department of social welfare in protest over a new departmental regulation requiring them to supply computers with "intimate facts" about the mental illness of their clients. The data was linked to the client's social security number.

54. Squires, B. E., Jr. Statement in [56].

55. Star, J. The computer data bank: will it kill your freedom? *Look* (25 June 1968), 27–29.

A short, very well-written popular survey of computers and privacy. Some well-detailed accounts of uses computer data banks are being put to today are presented.

56. U. S. Congress. The computer and the invasion of privacy—hearings before a subcommittee of the Committee on Government Operations, House of Representatives, 89th Congress, Second Session (Gallagher Report), U. S. Government Printing Office, Washington, D.C., 26–28 July 1966.

Pro and con on a national "statistical" data bank—the full testimony.

57. U. S. Congress. Computer privacy—hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate, 90th Congress, First Session (Long Report), U. S. Government Printing Office, Washington, D.C., 14–15 March 1967.

The full testimony before the Long subcommittee on computer privacy.

58. Warburton, P. Letter to the editor. *Comput. Automat. 16*,5 (May 1967), 8.

A "Resolution on the National Data Center and Personal Privacy" proposed by the Washington, D.C. Chapter of the Association for Computing Machinery is given.

59. Ware, W. H. Security and privacy in computer systems. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 279–282.

This is a general outline of the major vulnerabilities of time-sharing systems which handle sensitive data. It also served as an introductory paper for the session on privacy at the conference.

60. Watson, T. J., Jr. Technology and privacy. Speech given to Commonwealth Club of California, Hotel St. Francis, San Francisco, Calif., 5 Apr. 1968.

An address by the Chairman of the Board of IBM to the Commonwealth Club of California. Watson discusses in general what the privacy problem is, advantages and disad-

vantages of centralized data banks, and possible steps toward solving the problem. Suggestions are given for legal, ethical, and technological safeguards.

61. WEISSMAN, C. Programming protection: what do you want to pay? *SDC Mag. 10*,7-8 (July, Aug. 1967), System Development Corp., Santa Monica, Calif.

62. WESTIN, A. F. *Privacy and Freedom*. Atheneum, New York, 1967.

A comprehensive, well-written book on the relationship of privacy to freedom, tracing "privacy rights" from 1776 to the present. The emphasis is on the present and the future. The book has four parts: (1) the functions of privacy and surveillance in society, (2) new tools for invading privacy, (3) American society's struggle for controls (five case studies), and (4) policy choices for the 1970's. Each part is copiously documented, and in addition there are four bibliographies at the end: the functions of privacy, the new technology, the struggle for controls, and privacy in American law and policy. The section on computer technology and possibilities for it by 1975 is quite enlightening. Numerous legal decisions are cited in this seminal work. It is must reading for those seriously concerned with the general problem of privacy.

63. WESTIN, A. F. The snooping machine. *Playboy 15*, 5 (May 1968), 130ff.

A good review of initial and revised ideas on a national data bank. The advantages and disadvantages are set forth in this article in a nontechnical (!) publication. An interesting account of the automated adventures of a mythical citizen in 1975 is given.

64. BINGHAM, HARVEY W. Security techniques for EDP of multilevel classified information. Doc. RADC-TR-65-415, Rome Air Development Center, Griffiss Air Force Base, New York, Dec. 1965. (Unclassified)

The study objective was to develop hardware and software techniques for security (need-to-know) control of on-line users and programmers in multiprogramming, multiprocessing EDP systems of apparent future development. Hardware techniques recommended include: (1) processors having two modes of operation, interrupt entry into control mode in which privileged instructions are executable, flag bits for identification and control of memory words, and address checks against access-differentiated memory bounds; (2) parity checks on intermodule information transfers; (3) input/output control processors, which establish and verify peripheral unit connections, check memory addresses against bounds, and confirm security content of record headers being transferred; and (4) bulk file control of physical record integrity, and lock control over write permission and flag bit setting to permit supervisor establishment of control programs. Software techniques reside in the executive control program and are executed in control mode and identified by flag bits. Security routines are described and evaluated which construct, protect, and check access requests against user security control profiles, verify memory bounds and memory blanking, and provide security indicators for input/output. The integrated techniques are applied to control users and system programmers in an advanced modular system. Retrofit of most of the recommended techniques to an existing data processor (the Burroughs D825 Modular Data Processing System) is feasible. An external retrofit unit is described which provides control mode and privileged instructions for single-mode processors.—Author's Abstract

This paper is the final report of an eight-month study program conducted by the Burroughs Corporation for the US Air Force. It is a highly technical description of a proposed multiprogramming, multiprocessing, on-line computer system designed with security of information in mind. A very detailed report, it deals with technical aspects of a computer system operating in a secure environment; the report does not touch on cryptography, long-distance communications problems, electromagnetic radiation monitoring, physical security, equipment wiretapping or physical modifications, personnel problems, or administrative procedures.

Recommendations made by the study are described in the author's abstract above. In addition, the reviewer notes the following which may be of interest. Physical keys associated with a user are recommended (p. 7). The system requires the user (or an operator with a master key) to be physically present at a terminal before input or output can occur. An execute-only bit in each word is recommended (p. 9). This is turned on in routines of the operating system, thus guaranteeing its integrity.

The amount of hardware over and above that required for a traditional system is detailed in terms of "equivalent flip-flops" in Table 2, p. 56. Software security techniques are summarized on pp. 71–72. An attempt is made to gauge the costs of these techniques on pp. 99–100, the units of measurement being additional instruction executions necessary and additional storage space used. Ample justification is not given for these estimates, which tend to be plausible but low. A detailed description of startup procedures for this security-oriented system is given on pp. 77–80. Tables of all hardware and software security techniques which were considered in the study (not only the ones recommended), along with their application, what they protect against, and additional comments, are given on pp. 119–127. Pages 101–112 describe the detailed interfaces recommended for security between terminal units, bulk files, and the input/output control processor. Pages 113–117 detail retrofits (changes) necessary to implement the proposed system on the Burroughs D825 computer system, an existing multiprogramming and multiprocessing system. General flowcharts of key security routines are given in Appendix I. A brief discussion of the literature on error-correcting codes and redundancy techniques is given in Appendix IV. Pages 115 and 116 are switched

in this report of 173+xiii pages, which contains 12 illustrations, tables, and a glossary.

This report should definitely be read by all who plan to design or configure a computer system in which secure information must be protected.

65. Dueker, K. J. Data sharing and confidentiality in urban and regional planning. Proc. Urban Inform. Syst. Assoc. Fifth Annual Conf., Garden City, N.Y., 8 Sept. 1967.

A good overview for statisticians, urban planners, and the interested layman of the computer privacy problem. The first 15 pages present a good summary of the computer invasion of privacy literature. The latter 11 pages present implications of the National Data Center proposal to planners at the state and local levels. The latter part will interest urban planners particularly, while the former is of general interest. This easily readable paper is not at all technical. Some of the references do not exist in the volumes cited.

66. Evans, D. C., and Le Clerc, J. Y. Address mapping and the control of access in an interactive computer. Proc. AFIPS 1967 Spring Joint Comput. Conf., Vol. 30, Thompson Book Co., Washington, D.C., pp. 23–30.

An idea for extended segmentation hardware is presented. This hardware would control access paths at execution time, permit selective input and output operations under actual control of interactive users, and eliminate the need for relocation of programs at load time. Access control is by hardware at the segment level. The system has not been implemented, although "the hardware and software problems have been analyzed extensively," according to the paper, in the Ph.D. dissertation of the second author. The ideas on access control, whether eventually done in hardware or software, are steps in the right direction.

67. Sawyer, J., and Schechter, H. Computers, privacy, and the national data center: the responsibility of social scientists. *Amer. Psychologist 23*, 11 (Nov. 1968).

A paper for social scientists discussing the advantages to be gained by creation of a national data center and the pitfalls vis-a-vis privacy. The paper gives a good history of the proposal for a national data center and an excellent view of what stage the proposal is in currently (August 1968). It presents an excellent suggestion; namely, that only random samples of respondents be kept (one in 1000 samples are adequate for most analyses in the social sciences).

68. U. S. Congress. Privacy and the national data bank concept. House Committee on Government Operations. U.S. Government Printing Office, Washington, D.C., 2 Aug. 1968.

A very excellent review of the national data bank concept, which explains why such a system would be most helpful in certain areas and how it poses grave threats to privacy if not carefully designed. Initial actions by the Bureau of the Budget to study the feasibility of a central, computer-based data bank are reviewed very briefly, as are the hearings of the House of Representatives Special Subcommittee on Invasion of Privacy. The Committee on Government Operations notes that "the reports commissioned by the Bureau of the Budget do not contain well-thought-out theoretical or practical procedures necessary to insure privacy" and that the Budget Bureau "has not come to understand fully the importance of privacy in the National Data Center system." It suggests in detail procedures, safeguards, and alternatives to be considered in formulating specific proposals for a national data bank. These can be applied to *any* data base of sensitive information and should be quite carefully considered by designers of any such data bank, public or private. This 34-page document is a gem and an absolute must for those concerned with the specter of a national data bank.

69. Santa Clara (California) County. LOGIC User's Guide for Terminal Inquiry Systems. General Services Agency, Data Processing Center, Santa Clara County, Calif., 1 Aug. 1967.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 2

Privacy and Commercial Reporting Agencies

by R. Dale Gibson and John M. Sharp

"Privacy and the Law: Research Report No. 1"

Legal Research Institute of the University of Manitoba, Oct.1968

*****

DOCUMENT NO 2

Privacy and Commercial Reporting Agencies

par R. Dale Gibson et John M. Sharp

"Privacy and the Law: Research Report No. 1"

publié par le Legal Research Institute de l'Université du Manitoba, oct. 1968

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

PRIVACY and COMMERCIAL REPORTING AGENCIES

by

R. DALE GIBSON
Professor, Faculty of Law, University of Manitoba

and

JOHN M. SHARP
Assistant Professor, Faculty of Law, University of Manitoba

Privacy And The Law
Research Report No. 1

LEGAL RESEARCH INSTITUTE
of the
UNIVERSITY OF MANITOBA

WINNIPEG, MANITOBA
OCTOBER, 1968

CONTENTS

PREFACE

The Legal Research Institute of the University of Manitoba came into existence in May, 1968, after a committee, which included members representing the Faculty of Law of the University of Manitoba, the Government of Manitoba and the Law Society of Manitoba, had considered the desirability and the practicability of such a body.

It was felt that an Institute of this nature could serve a number of functions; it could not only co-ordinate legal research projects initiated within the Faculty of Law and the research work involved in these, but it could also work on specific projects or problems referred to it by private and public bodies outside the University organization. (The Faculty of Law had already participated for some time in the interdisciplinary studies, such as those on Transportation and Water Resources, being conducted in the University.)

Having been created on this basis, and operating under a Director who is a member of the Faculty of Law, the Institute approached three projects during its first six months of existence. The projects were a survey of the law of privacy, a history of the legal profession in Manitoba and a draft of a new Manitoba Court of Queen's Bench Act. Each of these projects, of which the first originated within the Faculty, the second was commissioned by the Law Society and the third by the Chief Justice of Manitoba, was approached by one or more professors with student research assistance.

This publication represents the first fruits of the group engaged in the study of the law of privacy. It is, of course, concerned with but one facet of the many involved, and will be followed by further publications.

It is intended that the Institute shall publish from time to time, and as an inter-related series, booklets such as this first one, which will set out the results of its work on particuar topics within the larger framework of the major projects. Eventually, much of the contents of these booklets will be incorporated in the major reports of the groups working on these projects.

It is hoped that two beneficial results in particular will flow from the publication of the Institute's conclusions in this way. One is that each booklet will deal with a specific topic, and consideration may be given to these in the first instance one at a time,

rather than as items swallowed-up in a larger mass. The second is that, in this way, criticism, support or opposition, may be engendered and communicated so as to be available for consideration before a final report is made.

Any comment on this or future booklets in the series directed to The Director, The Legal Research Institute of the University of Manitoba, Faculty of Law, The University of Manitoba, Winnipeg, will be received with interest and in the same spirit in which it is given.

JOHN M. SHARP,
Director.

INTRODUCTION

Credit bureaus and other commercial reporting agencies are important features of the modern commercial scene. These are organizations which gather and provide to their members or customers personal information about individuals and corporations in which their members or customers have some commercial interest (by reason of being prospective lenders, insurers, employers, etc.). The activities of some of these organizations are regarded by some observers as constituting an unjustifiably great intrusion into the privacy of the individuals being investigated.[1] They have recently come under the scrutiny of a sub-committee of the United States House of Representatives,[2] and legislation to regulate their operations will be introduced at the next session of the United States Senate.[3] Because their operations are so significant a part of the business world, and because their methods are currently under fire, reporting agencies were chosen as one of the first areas of inquiry for the privacy law study of the University of Manitoba's Legal Research Institute.

In the preparation of this report we were gratified to receive the full co-operation of the commercial reporting profession. Without exception, the major reporting agencies in the Winnipeg area granted us lengthy and completely frank interviews. These interviews, supplemented by considerable reading on the subject,[4] provided the factual basis for this study. In addition, we sent a preliminary draft of this report to each of the agencies, and received in return a number of valuable comments, several of which have resulted in significant modifications to the report.

---

[1] See for example, the testimony of Professor Alan F. Westin given March 12, 1968, before U.S. congressional hearing: *Commercial Credit Bureaus: Hearings before a Sub-Committee of the Committee on Government Operations, House of Representatives,* 90th Congress, 2nd Session, pp. 4 and 46.

[2] *Supra,* note 1.

[3] According to *Newsweek,* Aug. 19, 1968, p. 14, Senator William Proxmire will introduce remedial legislation at the next session of the United States Senate.

[4] *Commercial Credit Bureaus, supra,* note 1; Westin, *Privacy and Freedom,* Atheneum N.Y., 1967; Canadian Credit Institute, *Credits & Collections in Canada,* Ryerson, Toronto, 1958; Karst, "The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data", (1966) 31 Law and Contemporary Problems 342; Podell & Kirsh, "Credit Bureau Functions of Trade Associations: The Legal Aspects" (1927) 1 St. John's L.R. 101; Switkay "Tort Liability of Credit Investigating Agencies", (1957) 31

Temple L.Q. 50; McLennan, "The Bank and the Credit Bureau", The Canadian Banker, Winter 1961-2, p. 30; Niebergall, "Credit Information", The Canadian Banker, Summer 1966, p. 84; Quindry, "Credit Nerve Centers", (1938) Commercial L.J. 438; Lunay, "How's Your Credit?", Canadian Business, May, 1950, p. 38; Catherwood, "Your Credit Record Casts a Long Shadow", The Financial Post, Mar. 2, 1968, p. 23; Taylor, "To Your Credit or Not, Facts Are on File", Winnipeg Tribune, Dec. 18, 1967, p. 1; Morris, "What the Credit Bureaus Know About You", Reader's Digest, November 1967, p. 85; Donovan, "Security and 'Individual Privacy'", Security World, June 1967, p. 24, August 1967, p. 13, Sept. 1967, p. 29.

THE COMMERCIAL REPORTING PROFESSION

There are many different reporting agencies operating in most large cities, and no two agencies are exactly alike. It is possible, however, to classify them into two major types: those which basically act as information exchanges between groups of merchants operating in particular areas, and those which actively search for information on behalf of their members or customers. The former are often referred to as "file" agencies, and the latter as "investigating" agencies. The distinction is not an absolute one, however — companies which primarily carry on one kind of operation often at least dabble in the other.

In a typical file-type operation, the major credit grantors in an area (department stores, banks, finance companies, etc.) agree to make available to each other through the reporting agency the payment records and other credit information of those to whom they have granted credit. This type of operation is usually concerned exclusively or primarily with credit information. The "credit bureaus" to be found in most important centres in Canada and the United States fall into this category.

In some file operations the credit grantors simply supply specific information from their own files on request, but it is more common now for them to provide an automatic continuing input of data to central files maintained by the reporting agency. This information is usually supplemented by information relating to bankruptcies, divorces, criminal convictions, promotions, public service awards, etc., gleaned by the reporting agency from public records and newspapers. Many of these file operations are highly mechanized, with automated files and special telephones enabling merchants to obtain "verbal" checks on prospective customers within minutes. In the United States some of these operations are now computerized,[5] and in some of the Canadian agencies computerization is being actively studied.

The investigating agencies function in a much different way. When a request for information is received an employee actually investigates the matter by telephone or by personal interview. As with the file-type operations, this information is usually supple-

---

[5] Evidence of H. C. Jordan, President of Credit Data Corporation, *Commercial Credit Bureaus, supra,* note 1, p. 63. Evidence of John L. Spafford, Executive Vice-President, Associated Credit Bureaus of America, *ibid* p. 108. The only agency presently operating in Manitoba whose American parent is computerized is The Hooper-Holmes Bureau Inc.

mented by data from public records and newspaper clippings. The purposes for which the information is sought vary considerably — the assessment of applications for insurance (life, automobile, fire, etc.), credit, employment and bonding being the most common purposes — and so the sources of data also vary widely — the applicants, employers, neighbours, bankers, public records and so on. The reports of investigating-type agencies are generally submitted in writing.

We have made no attempt to estimate the total number of reporting agencies operating in Canada, but it must be very high. There seems to be a "Credit Bureau", or a branch thereof, in virtually every significant urban area in North America. In the United States more than 2,000 bureaus, serving 36,000 communities, are members of the Associated Credit Bureaus of America.[6] And in Canada, where they are linked by the Associated Credit Bureaus of Canada,[7] they seem to be just as common. There are, in addition, other file-type agencies competing with the credit bureaus, although competition is hampered by the reluctance of the principal credit grantors to co-operate with more than one pool, and by the policy of the Association to grant membership privileges to only one bureau in any one particular area.

Competition is more noticeable among the investigating-type agencies. Of the six reporting agencies that we studied in the Metropolitan Winnipeg area, two were file-type operations: the Credit Bureau of Winnipeg Ltd., which is primarily concerned with consumer credit, and Canadian Credit Men's Association Ltd., which is chiefly interested in credit granted to businesses rather than to individuals.[8] The other four agencies — Retail Credit Company of Canada Limited[9] (with which Retailers' Commercial Agency Inc. is affiliated), The Hooper-Holmes Bureau Inc., Progress Reporting Services Ltd. and Dun & Bradstreet of

---

6 Evidence of Professor A. F. Westin, *supra*, note 1, at p. 5; and evidence of John L. Spafford, Executive Vice-President, Associated Credit Bureaus of America, *ibid*, p. 105.

7 See N. K. Gateson, "Associated Credit Bureaus of Canada", in *Credits & Collections in Canada, supra*, note 4, p. 172.

8 See J. P. Sheffield, "The Canadian Credit Men's Trust Association Limited", in *Credits & Collections in Canada, supra*, note 4, p. 187.

9 See W. L. Fulghum, "The Retail Credit Company" in *Credits & Collections in Canada, supra*, note 4, p. 182.

Canada Ltd.[10] — are investigating-type companies, and although their areas of emphasis or specialization differ somewhat, they appear to be business rivals. In addition to the reporting agencies themselves, of course, a considerable amount of this type of work is done by private investigators, collection agencies, and by the credit grantors themselves.

Generally speaking, reporting agencies seem to be commercial enterprises aimed at producing a profit for their proprietors or shareholders, rather than co-operative associations designed to provide members with services at cost. The only organization of the latter type operating in the Winnipeg area appears to be Canadian Credit Men's Association.

Five of the six organizations that we studied have national or international connections. As has been mentioned, the various independently owned credit bureaus in North America are linked by the Associated Credit Bureaus of Canada and the Associated Credit Bureaus of America, with the result that the owners of the Winnipeg Credit Bureau (who, by the way, also operate bureaus in five other Manitoba centres) claim to be able to obtain a report on someone from most parts of the western world. There is a possibility, in fact, that the Canadian Association will, in the distant future, become a single company. Canadian Credit Men's Association is part of a nation-wide organization in existence since 1910, and having ties with the National Association of Credit Management of the United States. Retail Credit Company, the pioneer and giant of the reporting business, has been in existence since 1899, and has 308 branch offices and 1300 sub-offices throughout North America.[11] The Canadian branches of Retail Credit Company have, since January 1, 1968, been controlled by a Canadian corporation, Retail Credit Company of Canada Limited. The Canadian company is staffed almost entirely by

---

[10] The Dun & Bradstreet operation is something of a hybrid. Reports are based on special investigations by Dun & Bradstreet reporters, but they are made and received automatically and kept on file, whether or not a request for information is received. Like Canadian Credit Men's Association Ltd., Dun & Bradstreet is primarily interested in businesses rather than individuals, although individuals are sometimes the subject of reports — either because they are individual proprietors of businesses or because a personnel report has been requested for some special reason. The activities of this unique organization are well described by G. W. Shave, "Dun & Bradstreet of Canada Limited", in *Credits & Collections in Canada, supra*, note 4, at p. 198.

[11] Statement of W. Lee Burge, President, Retail Credit Company, before the Congressional Sub-Committee, May 16, 1968.

Canadians, but it is wholly owned by the parent American company,[12] and information is capable of being obtained from any part of the entire organization. The Hooper-Holmes Bureau Inc. is also an American company, about the same age as Retail Credit Company, and it also has branches throughout North America. Hooper-Holmes is one of the companies which has begun to computerize, but this has not yet had any effect on its Canadian operations. Progress Reporting Services Ltd. is the only Winnipeg reporting agency without national and international connections, and even in that case there is apparently some possibility that a national association of "independent" operators may be formed in the future.

Unlike most other industries dealing with sensitive matters vital to the welfare of large numbers of people, the reporting profession is almost free from government control or regulation. There are regulatory statutes in a few places[13] but in most areas, including Manitoba, there are no licensing requirements or even regulatory statutes.

Who has access to the information compiled by reporting agencies? There seems to be a fairly widespread misconception that, for a price, anyone may receive a report. This is not true. All of the agencies emphasize that they will provide services only for their members or subscribers, and that they are very particular about whom they accept for membership. The controls exercised differ widely from one company to another. One agency says that it will not take customers "off the street", except in the case of responsible people like lawyers. Another says that it refuses to deal with anyone, including lawyers, unless they are credit grantors. One agency says that it will only accept national or international companies as customers, but admits that it sometimes, as a favour, co-operates with governments and other responsible authorities

---

[12] A spokesman for the company pointed out in a letter to us that the parent corporation "has quite a number of Canadian shareholders".

[13] Ontario requires private investigators to be licensed — Private Investigators and Security Guards Act, S.O. 1965, c. 102 — but reporting agencies seem generally to be exempt by virtue of section 2(b):

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

seeking information.[14] Most agencies employ identification codes or other methods of ensuring that inquiries come from members only, and they all require their customers to agree not to allow the information to be used for unauthorized purposes.

There have been some hysterical things said and written about reporting agencies. Some commentators seem to regard them as "private Gestapo" operations which should be entirely abolished. We do not subscribe to these views, however. The reporting industry plays an extremely important role in the modern economy, and to prohibit its activities would, in our opinion, be foolhardy. However, these activities do involve serious risks to the privacy of individuals, and the purpose of this study is to examine these risks and to suggest methods of minimizing them.

The risks to which we refer are of two types:

a) the danger of inaccurate or misleading information being reported, and
b) the danger of accurate information being used for unjustifiable purposes.

Each of these problems will be discussed separately.

---

[14] Statement of W. Lee Burge, President, Retail Credit Company, before Congressional Sub-Committee, May 16, 1968.

The representatives of the reporting industry with whom we spoke all stressed the high degree of accuracy for which they strive and which they usually achieve. We do not doubt the sincerity of their opinions or the earnestness of their efforts; nor do we dispute the generally high quality of their work. Nevertheless, we remain convinced that, in spite of the many precautions taken, a significant risk of error or misunderstanding remains. This is inevitable in any operation where masses of data are transmitted through the agency of large numbers of people at a very rapid rate. Indeed, the industry does not attempt to deny this.[15]

The potential sources of error and misunderstanding are many. The informant may be mistaken; a clerical error in the books of a credit grantor may result in a delinquency being reported in a credit bureau's files, or an interviewed neighbour may pass on unreliable gossip. (Most agencies have a policy of confirming all derogatory information from interviewees by a second opinion, but the second neighbour may well have heard and believed the same gossip.) In rare cases the informant (or one of the informant's employees) may maliciously report false information about someone out of sheer spite. Errors of transposition or switched identity can occur in the transmission of information from informant to agency, or from agency to customer. The identity of persons with similar names can easily be confused. (One agency official said that errors were practically never made in reports, "except where the names get mixed up, of course.") Matters in dispute can create misleading impressions in necessarily terse reports; so if I refuse to pay for a deep-freeze because it is defective, it may show on my record as a simple payment delinquency. (It was suggested during the United States congressional sub-committee hearings that an "in dispute" category could be included in the report,[16] but it is doubtful that credit grantors could always be counted on to use this description when appropriate.) Material can be mistakenly placed in the wrong file by

---

15 "Yes; there is room for error, but I think it is very minimal as proven by the experience that 95 per cent of the people who apply for credit obtain credit easily and promptly. We receive very few complaints of mistaken identity, less than 1 per cent of all the reports, I would say." Evidence of John L. Spafford, Executive Vice-President, Associated Credit Bureaus of America, at Congressional Sub-Committee hearing, *supra*, note 1, at p. 109.

16 *Supra*, note 1, at p. 77.

a careless file-clerk and the error missed by a busy telephone reporter. Finally, although we are convinced that all the agencies we studied strive earnestly to achieve the highest possible level of accuracy, there will always be a substantial possibility, while the profession remains unregulated, of irresponsible persons setting up reporting agencies and conducting them in a careless manner.

There is no need to stress the very serious consequences that can flow from errors like these. Refusal of employment, insurance, or even credit can cause grievous injuries, both in the short and in the long run, to the individual concerned and to his family. Therefore, any steps that can be taken to reduce the incidence of error should be given the fullest consideration.

Not every inaccuracy has such dire consequences, of course. As the spokesmen for the reporting profession correctly pointed out, there are many opportunities for errors to be corrected or rendered innocuous, and for misunderstandings to be explained. Prospective credit grantors or insurers and employers do not wish to turn down applications unless it is absolutely necessary, so they often disregard an isolated derogatory item in an otherwise unblemished record. When they do reject an application, they sometimes state the reason, thereby giving the applicant an opportunity to set the record straight. Most reporting agencies are willing to discuss an individual's file or report with him (although most are reluctant to show the actual file report to him), and to correct errors, or to include in the file an explanatory statement by the individual. And, of course, the Law of Defamation looms in the background, enabling dissatisfied individuals to sue the agency. (In most parts of the United States reporting agencies can only be sued successfully if it can be shown that they acted maliciously,[17] but in Manitoba and most other parts of Canada this protected status — known as "qualified privilege" — applies only to non-profit co-operative operations[18] which, as we have seen, are not common.)

Unfortunately, however, these opportunities for correction do not afford entirely adequate protection. There are several reasons for this, but the most important is that in many cases the victims of the errors never learn that they have been made. Sometimes (as where an employer is privately considering whether to offer

---

[17] Switkay, *supra*, note 4.

[18] *MacIntosh v. Dunn* [1908] A.C. 390; *London Association for Protection of Trade v. Greenlands* [1916] 2 A.C. 15.

an individual a job or a promotion), they do not even know that decisions affecting their future are being made. Often they are not told the reason that their application has been rejected. Seldom are they told the source of the information. (The representative of one of the leading reporting companies admitted, after boasting that they received only two or three complaints of inaccuracy a year, that their customers are under contract not to expose the identity of the reporting company.) A sophisticated applicant might guess that a reporting company had been at work, but most people are unaware of the activities of the reporting profession (especially in non-credit matters) and, in any event, it would be difficult to guess which one of the several possible companies is involved. If a man does not know that erroneous information is being circulated about him, or does not know by whom it is being circulated, it is meaningless to say that he has an opportunity to correct the error or to sue.

It appears, therefore, that to provide adequate protection against reporting errors, the problem will have to be attacked on two fronts. First, steps will be necessary to ensure that all members of the reporting profession continue to meet the exacting standards of accuracy which the leading agencies have already set for themselves. Second, a satisfactory method will have to be found for bringing errors to the attention of those whom they concern.

The first goal could be effectively accomplished by means of licensing legislation. In our opinion, the reporting profession should be subjected to the same type of public supervision that is imposed on other professions with great potentiality for harm. A licensing scheme would ensure that all the reporting agencies provide adequate training for their employees and take all reasonable precautions against unauthorized disclosure. It would keep fly-by-night operators out of the field, and it would ultimately improve the profession's image in the eyes of the public. In our discussions with Winnipeg spokesmen for the reporting profession, we encountered no opposition and a surprising amount of actual support for this proposal.

A word should be said here about private investigators. Although we have excluded them from the ambit of this study, there is not much doubt that many of the problems that we are exploring arise also (sometimes in a more acute form) in connection with the activities of private investigators. It is probable that licensing is also called for in their case. It might be tempting

for a legislator to lump the two groups together for licensing purposes. It was stressed by some representatives of the reporting profession, however, that they would not like to see this happen, because they do not want their work to become associated in the public eye with what they regard as the sometimes unsavoury activities of private investigators.

The second goal — to bring errors to the attention of the subject — presents a more difficult problem.

Some improvement in the present situation could be brought about by a few relatively minor measures. For example, we can see no justification for the practice of some agencies in prohibiting their customers from disclosing the identity of the reporting agency to the subject of the report. This constitutes an impediment to the correction of errors, and we believe that it ought to be classified as unprofessional conduct by the licensing authority. Another method of increasing correction opportunities would be to publicize the reporting profession, its members, activities and complaint procedures, either by means of advertising by the individual agencies, or public announcements by the licensing authority. But while these suggestions would be useful, they would not be nearly adequate, in themselves, to bring reporting errors to the notice of the subject. A more comprehensive solution is called for.

The most frequently advanced proposal in this connection, and one which is being actively considered by American legislators,[19] would require reporting agencies to submit copies of their reports to the individuals concerned. When we discussed this proposal with representatives of the profession we found, not surprisingly, that they were unanimously opposed to it. We were of the opinion, until the preliminary draft of this report was circulated and commented upon by the profession, that this proposal represented the best possible solution to the disclosure problem. Since then, however, we have been persuaded by the objections of the profession that such an approach would create many practical difficulties. Some of the objections raised by the profession will be discussed below.

Some agency representatives pointed out that if favourable as well as unfavourable reports were sent, they would provide the recipients with evidence of good credit which, if fairly current, might be used to support new applications and thereby deprive

[19] Testimony of Professor A. F. Westin, *Supra*, note 1; proposed legislation of Senator Proxmire, *supra*, note 3.

the reporting agencies of business. This would probably not occur as frequently as was alleged, since most credit reports are inexpensive, and a credit grantor would be unwise to act on the proffered report without having it confirmed or up-dated by a second report. However, in the case of more complex and expensive reports, such as those prepared by Dun & Bradstreet, this danger would arise.

The view was expressed during the American congressional sub-committee hearings[20] that if duplicates of all reports were sent out in the mail, the risk of having the information fall accidentally into unauthorized hands would increase. This is undoubtedly true, although the risk of loss in the mail is so minimal that in our opinion even a doubling of it would not represent a very significant danger.

Probably the most serious concern of the profession is that a disclosure-law might deter their informants. Several spokesmen expressed the fear that "sources of information might dry up" — because the informants might either fear defamation actions, or simply not want their customers, employees, or friends to know that they have been "informing" on them. We are of the opinion that this problem, while serious, would not necessarily justify rejection of a disclosure law. In the first place, the file-type operations are much less likely to be affected than the investigating-type, since the commercial informants who feed data to the central pools are much less likely to be deterred. They know, through their legal advisers, that, unlike the reporting agencies themselves, informants are entitled to invoke the defence of "qualified privilege" against defamation liability.[21] And if their customers become upset at learning that their transactions are not being treated confidentially, they are not very likely to do anything about it, since they know that they will probably receive the same treatment from the competitor down the street. In view of the great benefits which the information pool provides, it is very doubtful that a disclosure law would inhibit the co-operation of this type of informant. In the case of private informers of investigating-type reporting agencies, the deterrent effect of the disclosure law is likely to be greater, but we doubt that it would be sufficiently great to hamper reporting operations seriously. In any event, if it proved to be a problem, it could be dealt with by not disclosing the sources of

[20] *Supra*, note 1, at p. 142.
[21] *Jackson v. Hopperton* [1864] 16 C.B. (N.S.) 829.

information contained in the report (or by expressing it in some form of code).

Another difficulty that a disclosure law would create would be a very large increase in the number of complaints and requests for explanation received by the agencies. At present the Winnipeg Credit Bureau handles about fifty complaints a week, and the other agencies handle only a negligible number. Under a disclosure law, complaints would probably reach an entirely different order of magnitude. Even just explaining the terse standardized language of the reports might be a time-consuming task, although an explanatory note on the report forms themselves would be very helpful. The consequences of this drastic change would be both beneficial and detrimental. On the positive side would be the many errors brought to light and corrected. On the negative side would be the expense of maintaining expanded complaint departments and the increased risk to the reporting agency of defamation actions. The cost factor will be discussed below. The problem of defamation liability could be handled in either or both of two ways: it could be translated to a cost factor by the use of defamation insurance (such as we found already in use by several agencies), or it could be minimized or virtually eliminated by a law allowing commercial reporting agencies to rely on the defence of "qualified privilege" which is open to their informants and to non-profit reporting agencies. The latter change would mean that the agency would be immune from defamation liability except in the case of malice. We are of the opinion that the defence of qualified privilege should be so extended, provided that the privilege should be lost if the agency refuses on request to correct errors, or at least to notify the recipients of reports that certain items are disputed by the individual concerned.

Surprisingly, representatives of the profession seldom mentioned cost as one of the reasons for opposing a disclosure law,[22] yet we contantly felt that the presence of that factor lurking unarticulated in the background. It is indisputable that a disclosure requirement would make the reporting operation somewhat more

[22] One spokesman, in commenting on our preliminary draft, did stress the cost factor, however: "If regulation forces the cost of reports upward, some businesses may resort to making their own inquiries. Such inquiries will not be handled as professionally as a reporting organization would handle them and consequently there may be less screening out of prejudice and error." The cost increase likely to result from the controls suggested in this report would not, however, be nearly high enough to have such an effect.

expensive. In the case of agencies that primarily use written reports, the problem would not be too serious; making and mailing an extra carbon copy of reports would likely cause only a slight increase in the cost of the reports. In the case of chiefly verbal operations, such as the typical credit bureau, however, the matter would not be quite so simple. Because it would call for an entirely new procedure to be instituted, the cost would be out of proportion to that involved in systems already employing written reports. This could possibly place the verbal operations at a disadvantage in comparison to written report systems. However, we understand that there is no significant competition between the two types of operation — they satisfy quite different needs — so it does not appear to us to pose an insuperable problem.

While we have tried to show that the objections to a complete disclosure law raised by representatives of the reporting profession are not as substantial as they are sometimes made out to be, we acknowledge that such a law would create many problems for the profession. Would it be possible to modify the disclosure proposal so as to achieve the same result but avoid these difficulties? Two possible modifications come to mind.

First, if reporting agencies were required to give notice only of unfavourable reports, the size of the task would be drastically reduced; about ninety per cent of reports are favourable. The problem of having favourable reports used as future references would also disappear. It is for these reasons, probably, that the disclosure law being considered by the American congressional sub-committee is restricted to derogatory reports. There would be grave difficulties involved in such an approach, however, the foremost being to arrive at a satisfactory definition of "unfavourable". How would a statement that a man has "average ability" be classified, for example? And the objectionable feature of a report may be not that it contains something derogatory, but that it fails to mention some highly favourable fact.

A second modification, which would avoid the most serious of the difficulties discussed above, would be to require only a simple notice that a report has been made, and that the subject may examine it at the agency's office. This approach was suggested during the course of the American congressional hearings.[23] It would not be as effective a means of notifying the subject as

[23] *Supra*, note 1, at pp. 142-3.

mailing him copies of the actual report, since most persons would not take the trouble to investigate the matter. Moreover, there would be many unnecessary visits to the reporting agency. Nevertheless, this approach strikes us as a reasonable compromise between the need to inform people of statements made about them and the need to protect the reporting profession from unduly burdensome restrictions.

No purpose would be served by spelling out all the intricate details of such a notification scheme at this stage, but it might be useful to describe how it would operate in broad outline. Whenever an agency made a report, written or verbal, on an individual or corporation,[24] it would automatically mail a notice to the subject. There would be some time limit within which the notice must be sent — perhaps one week from making the original report. Some authorities have suggested that it would be satisfactory if cumulative notices were sent only every three or six months.[25] This would certainly reduce the cost, but we do not recommend such a procedure, because the information would not reach the individual until it was much too late to do anything about it. In cases where the agency interviewed the subject himself as part of its investigation, the notice could be given to him at that time but we would not favour a purely verbal notice in such circumstances.

The notice would simply state that a report had been made about the subject to the inquirer (named)[26] and could be examined by the subject or his authorized delegate, on production of the notice and adequate identification, at the office of the reporting agency between certain specified times of the day. Telephone and mail inquiries would not be allowed. We believe that the inconvenience of having to attend at the agency's office would sufficiently deter frivolous inquiries, but if a problem of this type developed a small deterrent fee (50¢ or $1.00) might be charged by the agency.

---

[24] Strictly speaking, our study is concerned only with the privacy of individuals, but there seems no good reason why businesses should not also be protected from the risk of erroneous reports.

[25] This suggestion was made during the American congressional hearing: *supra*, note 1, at p. 142.

[26] No doubt some inquirers would be reluctant to have it known by the subject that they were investigating his background, but we believe that if this feeling were strong enough to deter them from making the inquiry, it would probably be the type of inquiry that should not be made in the first place.

When someone appeared at the agency, with sufficient identification, and requested to see the report about him, it would be shown to him. Where the report was verbal, he would be shown a brief written resumé. He would be allowed to make notes, but would not be given a copy of the report, and would not be allowed to make a photographic reproduction of it. If he desired assistance in interpreting the document, it would be provided. If he disputed some item, the matter would be discussed with him and, if he insisted, the agency would be obliged to inform the recipient of the original report that the subject disputed the item in question.

To protect informants from embarrassment, it might be wise not to identify them in the report shown to the subject initially. However, it would be necessary to disclose sources in circumstances where the subject had some legitimate reason to know them, such as where he had a reasonable suspicion that the informants had been malicious, or had breached a legal duty of confidence. Various methods could be devised for determining whether sources should be disclosed in a particular case. One method would be to provide that informants must be identified only if the licensing authority, in its discretion, agrees that the subject's request for such information is justifiable. The need to consult the licensing authority would deter most frivolous requests, so the number of informants whose identity was actually disclosed would be quite small, and no significant "drying up" of information sources could be expected to result.

By what sanctions would such a notification scheme be enforced? Several appropriate ones come to mind — fine, censure or suspension by the licensing authority, and loss of the "qualified privilege" defence to legal liability — so there can be no doubt that legislation of the type suggested could be made enforceable.

We recommend that a notification law along the lines described above be enacted. In our opinion it would provide the public with reasonable protection against the dissemination of erroneous or misleading information about themselves without unduly hampering the operations of an essential profession. It is true that a notification law would cause the cost of reports to rise a little, but the increase would not be excessive and, in our opinion, it is only fair that the reporting enterprise should bear the cost of the risks which it creates.

Truth is a dangerous commodity.[27] Even information which is entirely accurate is capable of causing grievous and unwarranted injury if used in a malicious or an unreasonable manner. Who would condone the publication of the previous criminal record of someone who is currently a pillar of his community? Who would justify the exposure of an unmarried mother posing as a widow to protect herself and her child from derision? In this section of our study we will be concerned with methods of preventing sensitive information about individuals from falling into unauthorized hands.

The controls that we will examine operate at two different levels. First, there is the problem of preventing certain kinds of information from getting into the files of the reporting agency in the first place. And then there is the question of making sure the data that is collected is not used for improper purposes.

One method of controlling the input of information to the reporting agencies would be to prevent them from gathering certain types of data altogether. Until recently it was common for reports to mention the subject's race. This information could be relevant (since certain racial groups are more susceptible to some diseases than others, it could be useful in establishing life insurance premiums for example), but it is so susceptible of abuse that most of the large agencies now refuse to mention the subject's race. (Most of them also refuse to report on religion or political affiliation.) One of the agencies operating in Winnipeg still includes racial information, but its spokesmen have stated that they are considering removing the question from their forms. There may be some merit in legislation prohibiting all agencies from acquiring racial, political or religious information, but we feel that it would be better to leave the matter to the self-restraint of the profession (under the watchful eye of the licensing authority, of course).

Another way to control the input of data to the reporting agency would be to place some form of restraint on the informants. To an extent, the law already does this by imposing, in some circumstances, a legal duty not to disclose confidential information. Unfortunately, because the common law grows slowly,

---

[27] "Truth, like all other good things, may be loved unwisely — may be pursued too keenly — may cost too much": *MacIntosh v. Dunn*, *supra*, note 18, at 400.

case by case, the law on this subject has not yet reached a sufficiently advanced state of development to permit a full description of the type of protection it provides to privacy.

So far, the courts have not recognized a general right of privacy. They have, however, attached to certain confidential relationships a duty of non-disclosure, enforceable by injunction or damages. Lawyers,[28] physicians,[29] bankers,[30] employees,[31] spouses[32] and others have all been held legally liable for disclosing confidential information acquired in those capacities, for example. But many other relationships remain in doubt. Is a university entitled to disclose information about its present and former students? May a prospective employer, lender or insurer make unauthorized use of information disclosed by applicants? Does it matter whether the information was expressly described as "confidential"? There are also many unanswered questions about the situations in which legal duties of confidentiality have already been recognized. For example, are banks, which undoubtedly must refrain from disclosing information about a customer's deposits, under a similar restraint so far as other transactions, like loans, with their customers are concerned? (It appears that banks usually — though not invariably — refuse to give information about deposits, but commonly pass on loan information. If, as may well be the case,[33] they are in breach of their legal duty in doing so, this could be a situation where the common law provides too much protection to privacy.) To what extent will the courts treat implied consent by the subject as a defence to liability?

No clear indication of the future judicial development of the law of confidentiality is likely until the doctrinal basis for previously recognized rights has been established. It cannot be contractual, because although the duty often arises from a contractual relationship, it seems to apply to non-contractual agents, and to lawyers and doctors who provide their services gratuitously. It is possible that future courts may adopt an analogy to bailment law, establishing categories of confidentiality varying in stringency according to the manner in which the informaton was obtained,

---

[28] *Taylor v. Blacklow* [1836] 3 Scott 614.
[29] *A.B. v. C.D.* [1851] 14 Dunlop 177. See Freedman, "Medical Privilege", (1954) 32 Can. B. Rev. 1.
[30] *Tournier v. National Provincial Bank* [1924] 1 K.B. 461.
[31] *Initial Services v. Putterill* [1967] 3 W.L.R. 1032.
[32] *Argyll v. Argyll* [1965] 1 All E.R. 611.
[33] *Tournier v. National Provincial Bank, supra*, note 30.

or that they may simply hold, borrowing from negligence law, that anyone will be legally liable for disclosures which a reasonable person, balancing the potential for harm against the justification for disclosure, would not make in the circumstances. Of course, a legislature impatient with such tortured reasoning and snail's-pace development of law, could simply take matters into its own hands and pass a statute creating a complete new privacy law.

So many intriguing questions of this kind arise that the subject of common law safeguards of confidentiality, and the question of whether a general law of privacy should be legislatively created, will be the concern of other sections of the Legal Research Institute's privacy study. At this point it is possible to say, however, that common law provides a measure of protection against breaches of confidence which, like defamation law, will only assist the victim if he is aware that a breach has taken place.

The dangers involved at the output stage are even more serious than those at the input stage. Even information which might be quite proper for the agencies or their clients to have can be the source of much unjustifiable harm if it falls into the wrong hands.

Most agencies are well aware of this danger, and have taken a number of precautions against it. Employees are under strict orders to treat all information in absolute confidence. Agencies try to limit their clientele to reliable firms, and in most cases require their customers to sign a contract agreeing not to pass the information on. Agencies which give information over the telephone usually employ some kind of identification code to prevent inquiry from outsiders posing as customers.

In spite of all these precautions, however, the opportunities for unwarranted disclosure are numerous. Given the large numbers of persons employed in the work, and the human proclivity to gossip, it is inevitable that some information will be leaked by agency employees. This problem may be more serious in the file-type operations, where employees tend to be younger and lower paid, and to turn over more rapidly than in the investigating-type agencies. The agency's clients probably constitute an even greater source of leaks. The number of employees with access to the information at that end is undoubtedly larger, and the restraints placed on their use of the information are probably not as stringent or as strictly enforced as they are in the agency itself. This would seem to be particularly true in the case of written reports, which carry the risk of disclosure until they are physically destroyed.

The risk of deliberate "tapping" of the agency's information is probably not great, but it cannot be overlooked; it would not be overly difficult for a determined person to gain information by learning and using a client's code number or employing some pretext. Professor A. F. Westin disclosed in his testimony before the congressional hearing that he obtained a report about someone simply by writing to a New York credit bureau in the name of the University and requesting the information as a favour to the University. Westin has been criticized for the "underhanded" way in which he obtained this evidence, but the fact remains that he has illustrated how simply an unscrupulous person may gain access to a reporting agency's files.

One type of disclosure which some people regard as improper and others do not is the supply of information by reporting agencies to government departments, such as income tax and internal security authorities. At the American hearing, some agencies stated that they regarded it as their patriotic duty to comply with all requests for information from government sources, while others stated that they regard such requests as a dangerous prelude to "big brotherism", and resist them until ordered by court subpoena to comply. Our attitude on this matter is that generally there is less risk of abuse of such information by government sources than by private business. There is, however, one complication in the Canadian context which should be commented on. Some of the largest reporting agencies operating in Canada are American companies or subsidiaries. One of these companies has announced in the United States that it does co-operate with government investigators.[34] If this company or others were to provide information about Canadians to United States government officials, it might be some cause for concern in this country.

Several different suggestions have been made concerning methods of minimizing the likelihood of harm from unjustified disclosure. One proposal being given serious study by the United States congressional sub-committee would require reporting agencies to obtain the consent of the subject before making any report. We do not favour this suggestion. It would slow down the work of the profession considerably, especially in the case of telephone operations. In any event it could be at least partially defeated by the use of standard form authorizations, signed together with

[34] *Supra*, note 14.

the application for insurance or employment or credit, and probably not even noticed by the applicant. We believe that adequate protection from improper disclosure can be provided in other ways without taking so drastic a step. As mentioned above, we would also disagree with any proposal to prohibit disclosure to government authorities not directly concerned with credit-granting, although a restriction on disclosure to foreign government officials might have some merit.

In our opinion, there are three steps that should be taken to protect privacy in this area. First, the licensing scheme proposed earlier would provide a means of ensuring that the agencies continue to observe the various precautions which most of them now appear to be taking. Second, the notification law suggested above would enable a person to learn of unjustifiable disclosures, and avail himself of such protections as the law affords. Finally, it may well be that the general law should be altered to create more extensive civil or criminal sanctions than now exist with respect to unjustified invasions of privacy. As has been mentioned, this latter point will be explored fully by another section of the Legal Research Institute's privacy study.

SUMMARY OF RECOMMENDATIONS

The following are the recommendations made during the course of this report:

1. Commercial reporting should not be prohibited. 13
2. The commercial reporting profession should be regulated by means of licensing legislation. 17
3. Arrangements by which customers of reporting agencies agree not to disclose the identity of the agency to the subjects of a report should be prohibited. 18
4. More publicity should be given to the existence, functions and correction procedures of reporting agencies. 18
5. The defence of qualified privilege should be extended to the commercial reporting professions. 20
6. Reporting agencies should be required to notify the subjects of all reports that a report has been made, and may be examined at the office of the agency. They should also be required, when subjects insist, to forward to the recipients of the original reports, notice that the subjects dispute certain items. Sources need not be disclosed unless the licensing authority so orders. 22
7. Permission of the subject should not be required before a report can be made. 28
8. Disclosure of information to officials of a foreign government should be prohibited but disclosure to Canadian government authorities should not be prohibited, at least until the question of creating a general law of privacy has been studied more thoroughly. 29

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 3

The Right to Privacy in Canada

by David A. Cornfield

an extract from the "Faculty of Law Review", vol. 25, 1967

University of Toronto

*****

DOCUMENT NO 3

The Right to Privacy in Canada

par David A. Cornfield

extrait de la "Faculty of Law Review", vol. 25, 1967

publiée par l'Université de Toronto

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

THE RIGHT TO PRIVACY IN CANADA

DAVID A. CORNFIELD*

A. Introduction

In 1890 an article in the Harvard Law Review[1] introduced the concept of a right to privacy into modern common law jurisprudence. Hailed as "the outstanding example of the influence of legal periodicals upon the American Law"[2], *The Right to Privacy* by Samuel D. Warren and Louis D. Brandeis provoked the majority of U.S. jurisdictions, by gradual stages, to recognize the right of privacy as a separate legal right, entitled to a substantial measure of protection. This has been a purely American development. In the 70 years between 1890 and 1960, there were at least 30 notes and articles written in U.S. legal periodicals supporting the existence of the right and commenting upon its development.[3] The only English discussion in that same period was written in 1931 by Winfield. There were no others.[4]

The first Canadian article on privacy was written in 1961. The year 1964 and the establishment of a committee by the Canadian Bar Association "to survey the invasion of privacy by technological or electronic devices" marks the beginning of a healthy debate on privacy which has recently slipped into high gear. The three years following 1964 have seen the introduction of numerous bills in our Parliament and legislature and the appointment of a Royal Commission on privacy in B.C.

This essay attempts to assess the privacy issue in a Canadian setting. It begins by showing that the recent concern in Canada over invasion of privacy is founded on the same threats to personal and group privacy as have been well documented in the U.S. While no one (even post-1964) has yet "paraded the horrors" in a Canadian context, these threats are not confined to the U.S. They exist here and will be paraded in the first part of this essay. By setting out these intrusive elements of life in Canada which are commonly labelled objectionable as "invasions of privacy" it is hoped to give the substance of the problem at the same time as illustrating that it is worthy of our attention. With the problem thus established, there is then a preliminary attempt to define the concept of privacy and the interests being protected.

While the threats to privacy flourish in both countries, any right to privacy is confined to the U.S. The study of Canadian law in the next part of this essay shows that such a right has practically no status here. While there is protection afforded to some aspects of privacy, the incidence of this protection is sporadic and does not cohere in any logical way. The historical background of privacy, set out immediately following, sheds some light on this present state of the law.

---

*David A. Cornfield, B.A. (Toronto, 1964), Third Year, Faculty of Law, University of Toronto.

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

[2]Prosser, *Privacy*, 48 Calif. L.R. 383 (1960) [hereinafter cited as Prosser, *Privacy*].

[3]Prosser, *Privacy* 389, n. 6.

[4]Fleming, *Torts* 569 (3rd ed. 1965).

In tracing it through the ages, it appears that invasion of privacy is really a new problem, characteristic of the twentieth century and particularly of the last twenty years. Considering the long-standing problems that this country is still wrestling with, it becomes less surprising that Canadian courts and legislatures have not yet propounded solutions to the invasion of privacy issue. Still, there is good reason to believe that legislation respecting privacy will be passed within the next year or two and, with this in mind, the final part of the essay is directed to an investigation of the features which such legislation might contain.

B. Invasion of Privacy — A Problem in Canada

The recent developments in sophisticated electronic eavesdropping devices, compilation and storage of computer data, and psychological mind probing are common knowledge in Canada today. Most people are aware that telephone wires can be tapped, that tiny radio transmitters can be concealed in olives and that miniature infra-red cameras can take photos in the dark. What they are not aware of, and cannot be aware of by the very nature of the activity, is that these and other intrusive devices are being used in Canada today to observe and record their activity at work, while shopping and in their homes. Private individuals, police, government and administrative agencies, and industry are all engaged in these practices. One U.S. supplier of electronic "bugs" revealed that his company had sold thirty million dollars worth of sophisticated listening equipment in 1965 and that 15% of this total — i.e. four and one-half million dollars — had been sold in Canada.[5] This sales figure from a single supplier should indicate that the use of electronic eavesdropping devices is not an isolated incident in Canadian life.

Snooping devices and services are readily available to anyone who wishes to use them. The very first electronics shop visited by this author was able to produce from its front display counter a miniature radio transmitter smaller than a cigarette package which was designed as a secret listening device. Easily concealed on the body, this tiny radio transmits a signal than can be picked up by an ordinary FM radio. Included as a standard accessory is a tiny microphone disguised as a tie clip. The cost: $30 — and the store had sold nearly a hundred at that price. The Toronto telephone book lists 36 firms under the heading of "Investigators" and several of these advertise that they specialize in industrial surveillance and closed circuit TV systems. The Retail Credit Co., which keeps data files on forty-two million people in the U.S., has an affiliate in Canada which does applicant background reports for finance companies, insurance companies, employers and landlords. This company's largest competitor is another U.S. subsidiary — The Hooper-Holmes Bureau. It would be wishful thinking at best to assume that these companies use different methods in Canada from those used by their American parent companies.

These devices and services are available and they are used. In 1961 Pierre Berton's column[6] reported that it had become common practice for car dealers to bug their salesrooms. Customers who say they need time to talk things over

[5] Toronto Daily Star, Aug. 31, 1966.
[6] *Id.*, Feb. 5, 1961.

are "left alone" in one of these rooms. The salesman then listens in on their private conversation and finds out exactly what features to stress and what fears he must allay. Canadian real estate firms and finance companies have been accused of this same practice.[7]

The television and film industry makes use of the same devices. An article by Douglas Leiterman in the Globe and Mail[8] reveals that television reporters are not above using subterfuge to approach within filming and recording range of their victims without the latter being aware that a film is being made. In one case a CBC man strolled through a political convention with a microphone wrapped in a newspaper and a small transmitter in his breast pocket. In another a woman reporter hid a microphone in a brooch. In both cases private conversations were picked up and synchronized with cameras taking pictures from one hundred feet away.

Husband-wife disputes and labour-management disputes are both areas where the new listening technology is put to use. The only wire tapping conviction ever obtained in Canada involved a Hamilton detective who was fined $25 under the Ont. Telephone Act for tapping the telephone of a woman at the request of her estranged husband.[9] This method of gaining evidence of grounds for divorce is not uncommon. It can take the form of tapping telephone lines to learn where the parties are to meet, or it can be the bugging of the premises where adultery takes place to get evidence of the adultery itself. In *Zein v. Zein*[10] the evidence of adultery in a petition for divorce was based on "eight tapes of a sound recording device".

Unions seem to be the special objects of electronic eavesdropping. In March 1964, the Bell Telephone Co. confirmed that the phone lines of Canada's Maritime Union Trustees had been tapped. In January of 1966 the Oil, Chemical and Atomic Workers Union in Port Credit discovered a bug attached to their office telephone just after signing a contract with British American Oil to end a seven-week strike. The most recent example is the bugging of an executive meeting of a pulp union in Vancouver — this time by a rival union. It was this particular event which sparked the appointment of a Royal Commission on electronic eavesdropping in British Columbia in November of 1966.

The incidents cited this far have all been examples of private or industrial use of electronic eavesdropping but that is not to say that the police abjure this tool. At various times in the past ten years practically every major police force in Canada from the R.C.M.P. on down has admitted using wiretapping and eavesdropping devices. In Edmonton the police force is authorized to tap telephones under a municipal by law. The R.C.M.P. has a two-weeks course to train its officers in the methods of electronic intrusion[11] and there have been suggestions that they maintain permanent wiretap installations in major hotels, enabling them to tap any room phone should a suspect book into that hotel.[12]

---

[7]Globe and Mail, Jan. 30, 1967.
[8]*Id.*, June 29, 1964.
[9]Star Weekly, Mar. 6, 1965.
[10]Zein v. Zein, 40 D.L.R. (2d) 224 (1963).
[11]*Parl. Deb.* (Commons) June 15, 1965, at 2418.
[12]Toronto Daily Star, Aug. 31, 1966.

The police contend that they need to use eavesdropping devices if they are to be successful in the battle with crime. This is difficult to dispute, but the following examples illustrate that the police do not always use the utmost discretion in their use of such devices and that there must be some controls upon police use. In the city of Saskatoon evidence came to light a few years ago that the only telephone used by prisoners in the city jail had been arranged so that the police could listen to and record conversations. This included people who had not yet been convicted, conversing with their lawyers in supposed confidence.[13] In Victoria, newspaper reporters uncovered the fact that city police headquarters had listening devices concealed in the cubicles where prisoners received visitors.[14] Still more objectionable were the plans for a police station revealed by authorities in Oakville in Jan. 1966. Not only were all cells to be equipped with hidden mikes and closed circuit television, but there would be no place in the building where an accused could confer confidentially with his lawyer. After public pressure, all three situations were corrected but this leaves unanswered the question of how many other police facilities are also bugged. Only three have been discovered but it may well be that when an accused in custody talks to his lawyer, a policeman is always listening to the conversation, taking advantage of the confidence between solicitor and client.

Invasion of Privacy — a Problem in Canada: Summary—

The objects of the preceding pages has been to show that this type of activity goes on in Canada and that if the Americans are justified in their concern, we in Canada have similar justification. At all times it should be kept in mind that eavesdropping activities are by nature secret. For every incident that comes to light it is not unreasonable to assume that there are another hundred which no one ever knows about. The very fact that so many cases get reported is indicative of the enormity of the problem.

C. The Concept of Privacy

The problem discussed thus far has been limited to electronic and technological intrusion on privacy. The language of privacy is used to cover a much broader range of situations. If a scandal sheet prints the intimate details of a couple's love life, they complain that their privacy has been invaded. If an advertisement falsely states that Mr. X. has endorsed a particular product, he makes the same complaint. If a flour company uses a young girl's picture to adorn their sacks of flour, she objects, standing on her right to privacy. All these people are insisting on what Warren and Brandeis defined as the "right to be left alone". Professor Fleming has expanded on this as follows:

> In its broadest sense, the interest involved is that of 'being left alone': to maintain one's intellectual and emotional personality free from offensive intrusion by conduct calculated to annoy and induce emotional distress.[15]

This definition is said by one school of thought to cover at least three and possibly four different kinds of invasion of different interests. Dean Prosser suggests

[13] *Parl. Deb.* (Commons), Feb. 24, 1967, 13472.
[14] Globe & Mail, Aug. 16, 1966.
[15] Fleming, *Torts* 568 (3rd ed. 1965).

that almost all the confusion in this area is due to a failure to separate these four forms of invasion:

1. Intrusion upon the individual's seclusion or solitude or into his private affairs. (This would encompass the electronic and technological intrusions.)
2. Public disclosure of private facts about the individual. (The couple exposed in the scandal sheet.)
3. Publicity which places the individual in a false light in the public eye. (The purported endorsement.)
4. Appropriation, for commercial advantage, of the individual's name or likeness. (The young lady's portrait on the flour sacks.)[16]

While these are all tied together with the common name of privacy, Prosser is of the opinion that they have almost nothing in common. Each is an interference with the right to be let alone, but the features of each are radically different.

> Taking them in order — intrusion, disclosure, false light and appropriation — the first and second require the invasion of something secret, secluded or pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves a use for the defendant's advantage, which is not true of the rest.[17]

It is to be noted that this thesis does not go unchallenged. E. J. Blousten, a professor of law at New York University, has objected to the splitting of the broad privacy right into "four *ad hoc* categories", contending that only one right is involved — that of inviolate personality.[18] It is submitted that Prosser's approach should be adopted for two reasons.

The first is that Prosser's approach might be used to convince a Canadian court to recognize a right to privacy in tort. This is developed at greater length below. The second reason is that the most urgent problem of privacy in Canada today revolves around intrusion. While disclosure, false light and appropriation may affect a few individuals, intrusion is turning the twentieth century into what has been called the "Age of the Goldfish Bowl".[19] The Blousten approach would require all four interests to be discussed at every stage. The Prosser approach permits us to deal with the real problem unclouded by a host of other issues.

D. Status of a Right to Privacy in Canada

1. *Tort Law*

The number of discussions of the right to privacy to be found outside of American legal periodicals has now risen to four. Winfield's 1931 article[20] has been joined by Brian Neill's article in 1962 Modern Law Quarterly,[21] a chapter

[16]Prosser, *Privacy*, 407.
[17]*Ibid.*
[18]Blousten, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. Rev. 962 (1964).
[19]Brenton, *The Privacy Invaders* passim (1964).
[20]Winfield, *The Right to Privacy*, 47 L.Q.R. 23 (1931).
[21]Neill, *Protection of Privacy*, 25 Mod. L. Rev. 393 (1962).

in Professor Fleming's "Law of Torts"[22] and an article in Canadian Bar Review by D.L. Mathieson.[23] All these writers agree 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. Neill put it this way:

> It can be stated with some confidence that English Law does not recognize "the right to be let alone". Personal privacy as such is not protected as a right, nor is there any correlative duty imposed on other persons to prevent them infringing it.[24]

The one possible exception to this all-encompassing statement is to be found in the Canadian case of *Robbins v. Canadian Broadcasting Corporation*.[25] In that case the plaintiff was a doctor who had written a letter to the producer of a television programme called "Tabloid" criticizing some features of the programme. A few weeks later, during a further edition of "Tabloid", the name and address of the doctor were displayed on the screen and listeners were invited to write or telephone to the plaintiff to "cheer him up". As a result the plaintiff was subjected to a barrage of offensive letters, telephone calls and "gifts" so that he was obliged to disconnect his telephone and suffered serious inconvenience and worry. One of the plaintiff's pleadings was that the defendant "knew or ought to have known that the said television broadcast and request would be a damaging invasion of plaintiff's privacy." The Quebec Superior Court found that the law governing the subject was article 1053 of the Civil Code. That article reads as follows:

> '1053 Every person capable of discerning right from wrong is responsible for the damage caused by his fault to another, whether by positive act, imprudence, neglect or want of skill.

The court found that the defendant's servants had committed a "fault" but that there was "no need to attempt any precise definition of this fault".[26] They awarded $3000 damages.

This decision clearly established that there is a right to privacy in Quebec. The decision was not based upon the occupancy of land or the holding of personal property — it protected privacy *per se*. It was sufficient for the plaintiff to prove what amounted to an offensive intrusion into his solitude and he obtained a remedy. Unfortunately the case, decided in terms of the Quebec Civil code, offers little guide as to the common law position in the rest of the Canadian provinces. As pointed out by Walton[27] there are significant differences between French civil law and English common law in their approach to tort liability. Whereas an English court thinks in terms of a list of nominate torts, the French civil law knows nothing of separate torts as we understand them. The French law is divided into responsibility for delicts — i.e. wrongs done intentionally; for quasi-delicts — i.e., wrongs done unintentionally; for the acts of others in

[22]Fleming, *Torts* 568 (3rd ed. 1965).
[23]Mathieson, *Comment*, 39 CAN. B. REV. 409 (1961).
[24]Neill, *Protection of Privacy*, 25 MOD. L. REV. 394 (1962).
[25]Robbins v. Canadian Broadcasting Corporation, 12 D.L.R. (2d) 34 (1957).
[26]*Id.*, 40.
[27]Walton, *The French Law as to the Right of Privacy*, 47 L.Q.R. 219 (1931).

certain cases; and for damage caused by animals or things under the defendant's control. In every action for damages for what we would call a tort, the French court has simply to decide whether 'fault' on the part of the defendant has been proved, and if so whether this fault has caused damage to the plaintiff.

> This difference between the two laws is, I think, not without practical consequences . . . Without either affirming or denying that the list of torts is now finally closed, I venture to suggest that an English court will be slow to admit a new one . . . A French court presented with a novel case of alleged 'fault' would not, I think, feel quite the same reluctance. After all, there are myriad forms of fault, and that a new type should turn up occasionally is only to be expected. They are in no way bound to bring the case under any of the familiar heads of categories of wrongs familiar to English lawyers . . . for no such categories exist in French civil law. The only question is whether the fault on the part of the plaintiff caused the damage.[28]

Thus, while the other provinces might be persuaded to follow *Robbins v. CBC*, the case by itself would be a very thin authority on which to base an action for invasion of privacy.

There are several obstacles in the way of establishing a right to protection from intrusion upon seclusion, solitude or into private affairs. The first is to be found in *Victoria Park & Recreation Grounds Co. v. Taylor*,[29] a common law decision of the High Court of Australia in 1937 where the plaintiff requested an injunction to restrain the simultaneous broadcasting of race results from a high platform built on land adjoining plaintiff's racecourse. In that case, Chief Justice Latham categorically denied the existence of a general right to privacy. It is submitted that Chief Justice Latham's statement should be treated as completely uncalled for on the facts and that privacy was not at stake at all. On the contrary, the plaintiff was complaining about the defendant's intrusion not into something private, but into a public spectacle which was open to anyone who paid the price of admission. It seems quite clear that no interest in seclusion, solitude, or private affairs was at stake — only proprietary rights in a performance held on private property. Thus the first obstacle should be relatively easy to surmount. An *obiter dictum* of an Australian court could hardly be binding on a Canadian court dealing with a true case of intrusion.

While no other court has ever positively denied the right to privacy, there have been numerous cases where pleadings framed in privacy have been rejected by English courts. These cases, presenting the second obstacle to establishing a right to protection from intrusion, are discussed in the articles by Winfield, Neill and Mathieson. It is here that Prosser's thesis may prove exceedingly useful. A close reading of these three articles reveals that the only cases dealt with by English courts which even remotely resemble Prosser's intrusion tort have been where a plaintiff wishes to restrain his neighbour from opening new windows which command a view of his premises. The fact that a remedy was refused in these cases[30] is quite consistent with granting a remedy in an eavesdropping case since the basis of the tort would be an offensive intrusion. The fact that opening a new window is not offensive should not change the offensive

[28] *Id.*, 220.
[29] Victoria Park & Recreation Grounds v. Taylor, 58 C.L.R. 479, 496 (1937).
[30] Fleming, *Torts* 570 (3rd ed. 1965).

character of electronic snooping. All other cases considered by these articles were examples of Prosser's last three categories. If there are in fact four interests involved in the general right to privacy, any rejection of remedies in non-intrusion cases should be irrelevant to the intrusion cases.

There is powerful support for this thesis that privacy involves interests other than that of intrusion. Foremost is Prosser's own stature. Even Blousten, who is attacking the theory, is moved to justify the need for such a critique as follows:

> Privacy began its modern history as a tort and Dean Prosser is by far the most influential exponent of the tort. His influence on the law of privacy begins to rival in our day that of Warren and Brandeis. His concept of privacy is alluded to in almost every decided privacy case in the last 10 years or so and it is reflected in the current draft of the restatement of torts.[31]

Fleming's discussion of privacy is also divided into intrusion, appropriation and a third category — Interest in Personal Dignity and Self Respect — which telescopes Prosser's third and fourth categories into one. He states:

> There are many interests in privacy. The term is generic rather than specific, and it is more helpful to analysis if these interests are discussed separately rather than indiscriminately across the board.[32]

The final obstacle in the way of a Canadian court affording protection against intrusion lies in the very newness of the issue. In view of the meagre discussion of the point, the lack of knowledge about the problem and the absence of crystallized viewpoint in society, a court would be perfectly justified in stating that this was a matter for legislation. In this age of massive government interference in all aspects of life, it can hardly be said that this would be an abdication of responsibility. In fact it is quite probable that legislation will soon be passed granting a civil remedy for invasion of privacy. Such a bill was introduced into the B.C. legislature in 1965 and subsequently dropped from the order paper for reconsideration.

The conclusion from all this seems to be that as of this date no English common law jurisdiction has recognized a right to privacy *per se*. The only Canadian province which provides a civil remedy for invasion of privacy is Quebec and this unique protection is based on the Quebec civil code. There is a slim possibility that Prosser and Fleming might be marshalled together to provide a court with adequate grounds to give protection in a clear case of the intrusion type of invasion of privacy, but it is more likely that a court would be inclined to wait for legislation. The next opportunity for a court to discuss the problem may come in B.C. where the Pulp and Paper Workers of Canada have issued a writ in the British Columbia Supreme Court against their rival, International Brotherhood of Pulp Sulphite and Paper Mill Workers, asking damages for invasion of privacy for the bugging of their union convention in November of 1966.[33]

---

[31]Blousten, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. Rev. 963 (1964).
[32]Fleming, *Torts* 569 (3rd ed. 1965).
[33]Toronto Daily Star, Jan. 5, 1967.

2. *Criminal and Quasi-Criminal Law*

I The Mails

The Post Office Act, R.S.C. 1952, c. 212, states in s. 41:

> Notwithstanding anything in any other Act or law, nothing is liable to demand, seizure or detention while in the course of post except as provided in this Act of the regulations.

The only provision in the present Act for the opening of mail is in s. 44 (1) and (2) which state:

> (1) All mail from a country other than Canada containing or suspected to contain anything subject to customs or other import duties or tolls or anything the importation of which is prohibited shall be submitted to a Customs officer for examination.
>
> (2) A Customs officer may open any mail, other than letters submitted to him under this section, and may cause letters to be opened in his presence by the addressee thereof, and where the addressee of any letter cannot be found or where he refuses to open the letter, the Customs officer shall return the letter to the Canada Post Office and it shall be dealt with as undeliverable mail in accordance with the regulations.

There are at present no regulations under the Post Office Act relating to the opening of letters.[34] There are regulations under the Penitentiary Act which permit persons in charge of federal institutions to open incoming and outgoing mail,[35] but in view of the unlimited language of s. 41 ("Notwithstanding anything in any other Act or law. . .") such regulations may well be *ultra vires*.

Other than the regulations under the Penitentiary Act, the present Canadian law appears to be that there is no power at all to intercept or open letters, even by police or government agencies. It is noteworthy that in the case of letters coming into Canada, the addressee has the option of having the letter left unopened and treated as undeliverable mail. Thus there is an absolute prohibition against intercepting communications made by mail. As will be shown, no other form of communications receives this measure of protection.

II Communications by Telephone

The only Federal statute which might be used to control wiretapping[36] is s. 25 of "An Act to Incorporate the Bell Telephone Company of Canada"; it reads:

> Any person who shall wilfully or maliciously injure, molest or destroy any of the lines, posts or other material or property of the company or in any way wilfully obstruct or interfere with the working of the said telephone lines, *or intercepts any message transmitted thereon* shall be guilty of a misdemeanor.[37]

There has never been any attempt to use this section against wiretapping. It is clear that the primary purpose of the section was to prevent damage to property and interference with service. Wiretapping, which does not injure the wires or interrupt the communication, was clearly not contemplated.[38]

---

[34]Chorney, *Wiretapping and Electronic Eavesdropping*, 7 CRIM. L.Q. 448 (1964-65) [hereinafter referred to as Chorney].
[35]*Parl. Deb.* (Commons), Mar. 10, 1967, at 13869.
[36]Golden, *Electronic Eavesdropping*, 1964 C.B.A., 46.
[37]STAT. CAN. 1880, 43 VICT., C. 67, s. 25.
[38]*From the Editor's Notebook*, 3 CRIM. L.Q. 426 (1960-61).

Only five provinces — Alberta, Manitoba, Ontario, Quebec and Nova Scotia — have any statutes or regulations which prohibit or restrain interference with telephones. The only comprehensive laws are to be found in Alberta and Manitoba.[39] No person in these provinces is permitted to use recording equipment to record telephone conversations unless that equipment is connected to the telephone by means of recorder-connector equipment which is supplied and installed by the telephone commission and which emits a signal when a message is being recorded. Violation of this provision is an offence punishable by a fine of up to $1000 or 3 months imprisonment or both. If unauthorized recording equipment is found set up in such a way that recordings might be made of telephone conversations, this is *prima facie* proof that it was being so used. Use of any listening device, operating by direct attachment, induction or otherwise is also prohibited with a penalty of up to $2000 or 6 months imprisonment or both for violation. Here there is another strong presumption to aid prosecution — possession of equipment capable of being used to listen to telephone conversations is *prima facie* evidence of a violation.[40]

There is one exception to the Alberta Act — an amendment to Edmonton's By-law 2295 (The Telephone By-law) passed in 1965 at the request of the Chief of Police which permits a magistrate to authorize the police to wiretap. This apparent violation of s. 23 of the Alberta Telephone Act is justified on the grounds that the Edmonton telephone system is owned by the city and not the Commission to which the Alberta Act refers; therefore that Act does not apply.

Alberta and Manitoba are the only provinces that deal with wiretapping and surreptitious recording expressly. Contrary to popular opinion, they are the only two provinces where the "beep" signal in recording equipment is a requirement of law. While the Bell Co. in other provinces makes it a practice to rent subscribers equipment with a built in "beep", there is no compulsion to do so. Significantly, we no longer hear the signal when listening to recordings of telephone conversations on the radio today as we did a few years ago. Nova Scotia, Ontario and Quebec have some legislation that might be used against wiretappers, but these sections were not originally directed to that problem and at best would be hit and miss in their application. The Nova Scotia prohibition against attaching "any instrument or apparatus to any conductor without the consent of the company" is buried in a section dealing with theft of telephone current or services.[41] Both Ontario and Quebec make it an offence for any person who has listened to or acquired knowledge of any telephone conversation not addressed to him to divulge the purport or substance of such conversation "except when lawfully authorized or directed to do so".[42] Note that listening *per se* does not constitute the offence — the contents must also be divulged. The penalties are small ($50 or thirty days or both in Ontario; $100 or 3 months or both in Quebec) and there are no presumptions to aid in prosecution.

---

[39]Golden, *Electronic Eavesdropping*, 1964 C.B.A. 46.
[40]Alberta Government Telephones Act, STAT. ALTA. 1958, c. 85, ss. 22-24, as amended by STAT. ALTA. 1965, c. 92, ss. 12-13; The Manitoba Telephone Act, STAT. MAN. 1955, c. 76, s. 36.
[41]The Rural Telephone Act, R.S.N.S. 1954, c. 255, s. 44.
[42]The Telephone Act, R.S.O. 1960, c. 394, ss. 111, 112; The Telegraph & Telephone Company Act, R.S.Q. 1964, c. 286, ss. 23, 24.

The discussion thus far has been purely academic. It lays out what the laws are and compares their effectiveness as written. As a practical matter it appears that they are all equally ineffective. An article by P. Sypnowich in the March 6, 1965, edition of the Star Weekly reported that there had been only one wiretapping conviction in all of Canada — a Hamilton detective was fined $25 under the Ontario Act in 1963. Other than two charges laid in Montreal,[43] I have found no evidence to dispute this. This should not come as too much of a surprise. Considering the nature of the activity and the absence of means of enforcement, even one conviction is a good record. This problem of laws against wiretapping and electronic eavesdropping and their enforcement will be discussed later in this article.

"Except When Lawfully Authorized or Directed to do so."

The Radio Act[44] and the Telegraph Act,[45] like the Ontario and Quebec Telephone Acts, have a prohibition against divulging the contents of private communications "except when lawfully authorized or directed to do so." This expression is not defined in the Act, any reported case, or the relevant Interpretations Acts.[46] In the absence of any such definition, a logical form of lawful authority might be a search warrant issued by a justice of the peace or a magistrate. With this in mind the Ontario Provincial Police approached the telephone company in 1947 to learn what their attitude might be to being served with a search warrant to permit police to trace calls. Bell was against any such interference with their operations but agreed to send a test case to court on the question. Bell and the Attorney-General's department devised a search warrant that might be used to authorize wiretapping and had it issued by a justice of the peace against a bookmaker. As agreed, Bell moved to quash the warrant and the case came before Chief Justice McRuer of Ontario's High Court.[47] He found as follows:

> . . . the purpose of the search warrant is to secure things that will in themselves be relevant to a case to be proved, not to secure an opportunity of making observations in respect of the use of things and merely obtain evidence. In this respect I think the warrant is defective and an order will go quashing it.[48]

Undaunted, the Chief Constable of Toronto sent a representative to appear before the Commissioners on Uniformity of Legislation requesting a recommendation that the Code be amended to permit a justice of the peace to issue a warrant authorizing wiretapping.[49] The telephone co. appeared to oppose this on several grounds including "infringement of private rights." The committee agreed with Bell and decided to make no recommendation.

With this avenue closed to them, the police have adopted another easier route to the same ends. The theory was enunciated in an article by N.M.

---

[43]Globe & Mail, Oct. 20, 1962; Toronto Daily Star, Aug. 19, 1966.
[44]Stat. Can. 1955, c. 57 s. 2 (1).
[45]R.S.C. 1952, c. 262, s. 6.
[46]Chorney, *supra* n. 31, at 449.
[47]Brief presented to the Select Committee of the Ontario Legislature on the Administration of Justice by the Bell Telephone Co. of Canada (undated).
[48]*Re Bell Telephone Co. of Canada*, [1947] O.W.N. 651, 655.
[49]Conference of Commissioners on Uniformity of Legislation, *Proceedings* 36 (1948).

Chorney, a law student articling with the Department of the Attorney General of Ontario.

> The members of the Royal Canadian Mounted Police are charged in s. 18 (*a*) of the RCMP Act, 1959 (Can.), c. 54 with the general duty "to perform all duties" assigned to them "for the prevention of crime" and "the apprehension of criminals and offenders". The OPP and members of municipal police forces in Ontario are similarly charged by ss. 43 (1) (*a*) and 47 respectively of The Police Act, R.S.O. 1960, c. 298.
>
> Until the power of police forces to use wiretapping devices in the course of criminal investigations is expressly defined and controlled by legislation . . it is possible that any member of a police force who is acting under his general statutory duty of criminal investigation may give . . . the required lawful authority or direction to disclose communications.[50]

This explanation of the phrase, in the absence of definition, is as good as any. One must give it some meaning and if there is no way a justice of the peace or magistrate can "lawfully authorize or direct" then who else can do so but the police themselves. In any event it is clear that the police do not feel themselves bound by any prohibition against wiretapping.

III Miscellaneous Provisions Affecting Privacy

(*a*) *The Radio Act*

None of the legislation cited above would have any relevance to electronic eavesdropping if it was not associated with a telephonic or telegraphic communication. Legislation which might be used to control the use of miniature radio transmitters is found in the Radio Act.[51] Section 5 of that Act provides that no one shall establish a "radio station" without a licence granted by the Minister of Transport, and "radio station" is defined as a station equipped with transmitting apparatus intended for any form of radiolectric communication. This might well be used by the Department of Transport to go after non-licensed miniature radio transmitters. In fact they do not. Department of Transport officials see their duty as covering the allocation of channels and the guarding against illegal use of channels. They have publicly stated that they are not concerned with the rights of the individual,[52] or with short range transmissions.

(*b*) *Peeping Toms*

Before the enactment of s. 162 of the Criminal Code, the Supreme Court of Canada held that the conduct of a "peeping tom" who went on private property at night and looked through a lighted window, was not an offence under the Code or at Common Law.[53] In response to this decision Parliament enacted the following:

> 162. Everyone who, without lawful excuse, the proof of which lies upon him, loiters or prowls at night upon the property of another person near a dwelling house situated on that property is guilty of an offence punishable on summary conviction.

For some reason the section has been framed in trespass. It would not prevent a man who was standing on his own property from using sophisticated optical devices to peer into his neighbour's home, or a landlord from spying on his tenants.

---

[50]Chorney, *supra* n. 31, 449.
[51]R.S.C. 1952, c. 233, s. 5 as amended by STAT. CAN. 1952-53, c. 48, s. 11.
[52]THE TORONTO TELEGRAM, Mar. 6, 1965.
[53]Frey v. Fedoruk [1950], S.C.R. 517.

Still it does provide some protection from invasion of a person's seclusion, solitude and private affairs.

(c) *Indecent Phone Calls*

S. 315 (2) provides as follows:

> Everyone who, with intent to alarm or annoy any person, makes any indecent telephone call to such person is guilty of an offence punishable on summary conviction.

The first attempts to enforce this section have come within the last year. The phone company has taken a number of large advertisements instructing its subscribers in how to deal with crank calls and have placed a specially equipped detail of its employees to trace their source. There have been a number of convictions. Note that it is not sufficient that the calls be annoying or alarming. They must be indecent as well if all elements of the crime are to be shown.

(d) *Securities Legislation*

Like any other interest, the interest in privacy must face and be weighed against competing interests. One of these competing interests has already been mentioned — that of combatting crime. Another is the need of an expanding country for an orderly securities market where new ventures can be financed. The market will not be orderly if the investor has no information on which to base this investment decision and must rely on rumours. Thus the legislature has seen fit deliberately to encroach on areas of business which have been traditionally treated as strictly private. Companies are now required by law to make disclosures about their financial stability as an on-going business venture and soon insiders will be required to make public all their trading in their company's securities.[54] These are both invasions of privacy and yet desirable developments in our law.

IV The Courts

(a) *Admissibility of Evidence Obtained by Wiretapping*

There is little doubt that evidence obtained by wiretapping would be admissible in a Canadian court, even if illegal as in violation of an Act prohibiting wiretapping. While admittedly *obiter*, Mr. Justice Freedman of the Manitoba Queen's Bench dealt with this point in the case of *R. v. Foll.*[55]

> . . . even if the tape recording represented evidence illegally obtained as being in violation of the Manitoba Telephone Act (and I have already found to the contrary) it would still be admissible if relevant.

In support of this he cited *A. G. Que. v. Begin*[56] where the Supreme Court of Canada expressly adopted the rule of admissibility as formulated by the Privy Council in *Kurama v. The Queen*:[57]

> The test to be applied in considering whether evidence is admissible is whether it is relevant to the matters in issue.

---

[54]The Securities Act, 1966, STAT. ONT., 1966, c. 142, Parts XI and XII.
[55]R. v. Foll, 117 C.C.C. 19 (1956).
[56]A.G. Que. v. Begin [1955], S.C.R. 593, 595.
[57]Kurama v. The Queen [1955], A.C. 197.

Mr. Justice Freedman also considered the danger of tape recorded evidence having been tampered with. He held that after a *voir dire* to establish the accuracy of tape recordings, they would be admissible as evidence.[58]

(*b*) *Privileged Communications*

A characteristic of our judicial system is that disputes are settled in proceedings which are open to press and public. Witnesses can be compelled to disclose in this open court all facts in their knowledge which may be relevant to the issues, no matter how embarrassing, private or confidential. Such trials intrude upon privacy every day. The law has recognized this aspect of the trial and has declared that a right to privacy shall prevail in a few limited instances. Under s. 427 of the Criminal Code, the trial of a juvenile is directed to be without publicity. Communications between husband and wife, and solicitor and client are privileged and cannot be compelled in a court. The Quebec civil code (art. 275) makes the same provision for priest-penitent communications, and, while the common law has uniformly denied such a privilege, the courts are not anxious to compel this kind of evidence. In Ontario the general practice has been for the trial judge to suggest that questions of this nature be not pressed and there is no known instance where the suggestion has not been acceded to.[59] The law recognizes no privileges for doctor-patient communications[60] or a newspaperman's sources.[61]

(*c*) *Arbitration*

Parties who cannot settle a dispute themselves are not always forced to take it to an open court. Arbitration, as embodied in Ontario's Arbitrations Act,[62] offers an alternative. It permits parties to refer any dispute to an arbitrator who must then proceed in accordance with the terms of the submission. The parties to a submission can *sub poena* witnesses[63] and the arbitrator is given the power to administer oaths.[64] The hearings can be and usually are closed proceedings. Of course speed, expertise and absence of *stare decisis* are all considerations when parties elect arbitration, but a limited amount of privacy is certainly one of the inducements.

V The Right to Privacy in Canada: Summary—

The law affecting privacy in Canada ranges in effect from deliberate encroachments on privacy to a hit and miss protection. At least two of the factors which invade our privacy are, quite properly, institutionalized — i.e. securities legislation and the open court. The effect of the open court on privacy has been mitigated somewhat by privilege and the alternative of arbitration, but, unavoidably (and perhaps excessively), it is still intrusive. Two of the greatest threats to privacy are not controlled at all, miniature radio transmitters and

---

[58]See generally Chorney, *supra* n. 31.
[59]7 C.E.D. 334 (2nd ed. 1952).
[60]*Ibid.*
[61]Wismer v. MacLean-Hunter Publishing Co. Ltd. & Fraser (No. 2) [1954], 1 D.L.R. 501.
[62]R.S.O. 1960, c. 18.
[63]*Id.*, s. 14.
[64]*Id.*, s. 9 (*a*).

eavesdropping not associated with telephones. The only absolute protection afforded by the law to privacy is limited to communications by mail. The same information conveyed by telephone is private in only two province — Alberta and Manitoba. Three provinces have legislation which can be distorted so as to prosecute a wiretapper, but they can hardly claim to have consciously dealt with the matter or that the legislation is at all effective. Finally, with the exception of Quebec, there is presently no right to privacy *per se* in Canadian tort law and there is little prospect of convincing a common law court to alter the *status quo*. If there are to be any changes in this picture, they will have to be made by legislation.

E. Background

1. *Historical*

Thus far we have established that, in spite of massive intrusion on individual and group privacy in this country, there is a dearth of law and jurisprudence on the subject. To develop reasons for this requires some knowledge of the history of privacy in society.

An article by a sociologist at the University of Chicago gives us some of this history.[65] Professor Schils points out that when the greater part of the civilized world was located in tropical countries, heat, populousness and poverty caused much of daily life to be lived out of doors and much of indoor domestic life to be lived in conditions of severe over-crowding. Invasion of privacy was not a problem since there was no privacy to invade. There was little improvement when men moved indoors. Village life offered few distractions other than the affairs of one's neighbours and, with only a small number of people in any one place, every variation in one's life was noticed, scrutinized and interpreted so that each knew the other's affairs.

The coming of modern urban life marked the real beginning of privacy. Better transportation meant contact with large numbers of people and less interest in one's neighbour. Better education and communication meant that more interesting matters occupied one's mind. As crowded tenements gave way to private homes, privacy became a fact for large segments of the population and as the opportunity for privacy increased, respect for privacy also increased.

At the same time there was a corresponding growth in the elements which would intrude on this new-found privacy. While the proportionate amount of privacy had never been so large, the incidents of invasion had never been so disturbing. Yellow journalism took the place of backyard gossip and yet was more insidious than gossip since gossip had been taken with a grain of salt while anything in black and white seemed necessarily true. Independently organized bodies of police and private investigators began to specialize in undercover work against unions or rival companies. Psychologists became able to probe the mind and as corporations grew and became more impersonal, they were attracted by what seemed to be efficient, scientific methods of hiring.

---

[65]Schils, *Privacy: Its Constitution and Vicissitudes*, 31 Law and Contemp. Prob. 281 (1966).

These developments were well under way in the United States when Warren and Brandeis wrote their famous article. The eastern seaboard was rapidly becoming the urbanized and industrialized society which brings privacy and the invasion of privacy. Canada, on the other hand, was still a backwoods society of farms, towns and villages. Almost 70% of Canada's population in 1891 was living in rural areas.[66] Interest in privacy would not have the same relevance for another forty years. It is little wonder then that Canada has been devoid of jurisprudence or legislation for so many years following Warren and Brandeis.

2. Recent Developments

In June of 1964 the man who since became Solicitor-General of Canada, The Honourable L. T. Pennell, introduced a private member's bill to amend the criminal code to prohibit wiretapping and require police to obtain the consent of a judge of a superior court of criminal jurisdiction before intercepting telegraphic or telephonic communications.[67] The bill was re-introduced on April 8, 1965[68] but in neither case did the bill reach a second reading. The same bill was again introduced by an NDP and a Liberal member on Jan. 24, 1966.[69] Mr. Orlikow's bill, C-33, was identical to the Pennell bill. Mr. Stanbury's bill, C-45, substituted "private communication" each time "telephone" or "telegraph" appeared so as to cover any electronic or mechanical eavesdropping, not just those associated with the telephone or telegraph. Both these bills have recently been moved for second reading and been talked out.[70] In both cases, all members who spoke, while criticizing the details, approved the principle of the bills. The reason given for delay was that Parliament should wait until the Royal Commission on Security hands down its report. Two further bills have been introduced within the last few months — C. 269[71] and C. 273.[72] These bills originate with NDP members and are much broader than the Pennell model. C. 273 is the first bill to be drafted as a separate "Act Respecting Privacy" and not as an amendment to the criminal code.

The Solicitor General and the Minister of Justice have repeatedly stated, in answer to questions, that the matter is under consideration.[73] A Liberal member reports that the Department of Justice has received a number of recommendations on wiretapping and electronic eavesdropping. The Bell Telephone Co. has urged legislation and offered its cooperation and the Canadian Association of Police Chiefs is pressing for express permission for police to wiretap. At a conference of attorneys general in January, 1966:

> The attorney general of Saskatchewan advised that legislation in relation to wiretapping has already been prepared in that province and that the government intends to proceed with the legislation at this present session of the legislature. He left open, however, the possibility of federal legislation as a preferable solution.

---

[66]Porter, *The Vertical Mosaic* 138, Toronto: University of Toronto Press (1965).
[67]*Parl. Deb.* (Commons), June 4, 1964, at 3922. Bill C-103.
[68]*Id.*, April 8, 1965, at 93. Bill C-72.
[69]*Id.*, Jan. 24, 1966, at 139.
[70]*Id.*, Feb. 24, 1967, at 13472 and Mar. 10, 1967, at 13865.
[71]*Id.*, Feb. 16, 1967, at 13101.
[72]*Id.*, Feb. 24, 1967, at 13483.
[73]*Id.*, Feb. 2, 1966, at 568; May 17, 1966, at 5219; Nov. 9, 1966, at 9735; Jan. 20, 1967 at 12036; and Feb. 9, 1967 at 12880.

A number of provinces expressed themselves as being in favour of wiretapping legislation, these being Quebec, New Brunswick, Manitoba, Prince Edward Island, Alberta and Newfoundland.[74]

As mentioned in the introduction, a Royal Commission in British Columbia is presently holding hearings on the new techniques of surveillance, and testimony before that Commission is already indicating that electronic invasion of privacy is more prevalent than most had realized. British Columbia is also considering a bill which would create a remedy in tort for invasion of privacy. Such a bill was introduced by the B.C. government in 1965, but was dropped from the order paper for further study.

F. Legislation to Protect Privacy: Considerations for a Draftsman

This essay makes no attempt to assess the value of privacy or to weigh it against competing interests.[75] Ideally the role of privacy in shaping personalities and institutions would be extensively studied before any conclusions were reached, but since this is not an ideal world, and since there is a strong chance that legislation will soon be put on the statute books, it will here be assumed that privacy is worth protecting and the discussion will proceed to the problems faced in drafting legislation.

The draftsman should first be aware that the word "wiretapping" only refers to the direct, physical attachment of a listening device to a wire. It does not cover devices which merely touch the surface of the wire, and operate by induction. He should keep in mind that surreptitious surveillance is not limited to the interception of communications but can be carried out by hidden cameras and closed circuit television. The biggest problem will be to write a law that can be enforced. An American writer[76] has suggested that all owners of buildings and their employees be required to report the use of listening devices on their premises with a $250 fine for failing to report. The rationale of such a positive duty to report is that an owner of a building has control over that building and his knowledge amounts to wilful acquiescence. Another possibility would be to offer an incentive to voluntary reporting such as one half of any fine to be paid to the informer. This is a device which has been used in legislation in the past. The draftsman might decide to provide *prima facie* presumptions of guilt from proof of possession of electronic listening equipment, similar to the presumption found in the Manitoba and Alberta Telephone Acts. Before doing so, he should consider carefully whether the circumstances warrant shifting the traditional burden of proof.

There is little doubt that one of the draftsman's instructions will be to write in an exception for the police. This still leaves him some scope. He can set the degree of difficulty of obtaining consent at a high or low level: "from a judge of a Superior court of criminal jurisdiction" or "from a magistrate or justice of the peace". He might hedge in the court's discretion by specifying the kinds

[74] *Id.*, Mar. 10, 1967, at 13870.
[75] See generally Westin, *Science, Privacy and Freedom* (Parts I and II), 7 Colum. L. Rev. 1003, 1205 (1966).
[76] Swire, *Eavesdropping & Electronic Surveillance*, 4 Harv. J. on Legis. 23 (1966).

of cases where permission may be granted. The bills modelled on Mr. Pennell's c. 103, for example, only permit the police to eavesdrop where there are reasonable grounds to suspect an indictable offence punishable by imprisonment of ten years or more. If this type of restriction is to be imposed, it should probably be supplemented by a list of specific cases where eavesdropping is necessary but would not be covered by the ten-year requirement — e.g. gambling offences and prostitution offences, where the telephone is used in committing the crime. Another valuable limitation is to limit the consent which can be granted to a specified time period, requiring a renewal at that time. This has also been built into the three Pennell type bills.

If enforcement is a problem in the case of private wiretapping, it is twice as difficult a one in the case of the police. It is not hard to see that a policeman will rarely stand accused of using illegal tactics since this would require his fellow police and his collaborator, the crown attorney, to turn on him. The draftsman will have to consider if it is possible to keep the police within the formalities of the exception. The only answer seems to be to change the rule regarding evidence illegally obtained. While excluding such evidence is not a punishment in any sense, it does remove the incentive for obtaining evidence illegally. Here it would be useful to study the U.S. experience with the exclusionary rule for its effect on law enforcement. Prior to the decision of *Mapp v. Ohio*,[77] there were still some states where illegally obtained evidence was admissible. A study by L. B. Schwartz indicates that there was no noticeable difference in efficiency of law enforcement between states that admitted such evidence and states that did not. "On the contrary, the most effective and respected law enforcement agency, the F.B.I., operated under the long-standing federal exclusionary rule."[78]

The question of what can be done constitutionally is not a major problem. It seems quite clear that eavesdropping and other intrusions could be dealt with federally under the criminal law power, with the exception of the creation of a tort remedy which would be a provincial matter under property and civil rights. This at least is the stand taken in a brief which will soon be presented to the B.C. Royal Commission by the B.C. subsection of the Civil Liberties section of the Canadian Bar Association.

Conclusion

This essay has been very limited in its scope. It has dealt with only one area of privacy-intrusion into seclusion, solitude or private affairs and has done so strictly within a Canadian context. It has shown that this form of invasion of privacy is a real threat in Canada and that there are very few protections for privacy in the statutes or the common law. There has been an attempt to explain this state of the law and to illustrate the choices before a lawmaker in drafting legislation to prevent intrusion. If the recent debate is any indication, legislation may soon make most of this discussion obsolete.

[77]Mapp v. Ohio, 367 U.S. 643 (1961).
[78]Schwartz, *Excluding Evidence Illegally Obtained*, 29 Mod. L.R. 635, 638 (1966).

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 6

Legal Safeguards to Insure Privacy in a Computer Society

by Alan F. Westin

an extract from "Communications of the ACM", September 1967

*****

DOCUMENT NO 6

Legal Safeguards to Insure Privacy in a Computer Society

par Alan F. Westin

extrait de la revue "Communications of the ACM", septembre 1967

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

SPECIAL REPORT

Legal Safeguards to Insure Privacy in a Computer Society

By ALAN F. WESTIN,* *Columbia University, New York*

From the earliest days of the American Republic, our legal and political system has been devoted to placing limits on the powers of surveillance that authorities can conduct over the lives of individuals and private groups. This tradition of limiting surveillance goes back to a stream of development in Western history that begins at least as early as the democratic Greek city-state and represented one of the keystones of the American Constitution.

When the Framers wrote, physical surveillance over individuals and groups was possible only in terms of actual entry onto property, eavesdropping on conversations by ear, and overlooking individuals. To place limits on these forms of surveillance, the American Constitution required that searches and seizures by government be "reasonable," describing specifically the places to be searched and the persons or things to be seized. Reasonableness was determined by a judicial inquiry in which law enforcement officers had to establish probable cause and were examined by a judge about the scope and conduct of the inquiry.

When the Framers wrote, psychological surveillance over individuals was possible only by torture to extract information or beliefs, or proceedings to compel individuals to testify against themselves. To meet these threats to psychological security, the American Constitution forbade torture and self-incrimination.

The other remaining form of surveillance known to 18th century life was the record and dossier system maintained by European monarchies to control the movement of population and the activities of "disloyal" groups. In the United States, the openness and mobility of our frontier system and the deliberate refusal to employ a passport and dossier system of police control guaranteed that the American citizen would be free from these means of surveillance over his life.

Until the late 19th century, this legal framework was thoroughly adequate. The reasonable search and seizure principle allowed the balance to be struck by the courts and legislatures between the individual and group claims to privacy on the one hand and the needs of law enforcement and government information systems on the other. Then, late in the 19th century and accelerating rapidly during the first half of the 20th century, technological developments began to erode the legal system for guaranteeing a libertarian balance of privacy. The invention of the telephone in the late 1880's meant that conversations were now projected outside the home and a network of wires, conduits, and central offices contained the speech that originated in one private place and was meant for reception in another. Telephone tapping by police and private adventurers began virtually simultaneously with the installation of telephone systems in the United States, just as telegraph tapping had begun in the 1850's when the telegraph first became an important means of communication. At about the same time, in the 1890's, the microphone was developed and quickly applied to the problem of monitoring speech through surreptitious devices. The law enforcement agencies and the Pinkerton Detective Agency made "dictaphone detection" a by-word of the late 1890's and the pre-World War I era. With these developments, the erosion of physical boundaries on which the reasonable search and seizure concept of the Constitution had been based began to create stress in the application of Constitutional protections to privacy from physical surveillance. During the same period, advances in techniques of psychological surveillance also grew. The polygraph, developed in the 1920's, provided means of measuring the physical states and emotional responses of

Presented before the 1967 Spring Joint Computer Conference of The American Federation of Information Processing Societies, Atlantic City, New Jersey, April 18, 1967

* Professor, Department of Public Law and Government

individuals under stress, and this was picked up by both law enforcement agencies for questioning suspects and by private employers for investigating business employees and business crimes. Paralleling the polygraph development was the spread of deeply probing psychological tests of personality. Using a variety of approaches, from sentence completion and multiple choice tests to projective tests of situation and picture interpretation, psychologists applied measures of emotional adjustment and personality traits to the selection of individuals for a variety of purposes in governmental and corporate life. On the whole, American law drew a simple line in these areas—it forbade the use of polygraph or personality test results as legal evidence in courts but did not interfere in any way in the use of such tests for personnel selection and other non-judicial decision-making by authorities.

In the area of data surveillance, American society began the expansion of records and information keeping in the period between World War I and World War II, events which represented the natural outcome of an industrial society with a growing regulatory and welfare function by government and an increasingly large bureaucratic structure in private organizational life. For the most part, American law dealt with this problem by setting general standards of confidentiality for information given to government agencies under compulsion of law (such as census data, social security information, and income tax records). However, the prime protection in this area remained the inability of government agencies and private authorities to use the mountains of information they had secured in anything like a centralized and efficient fashion.

Now, the contemporary era of electronics and computers has provided the final coup de grace to the technological premises on which the classic American law of privacy has been based. Micro-miniaturization, advanced circuitry, radar, the laser, television optics, and related developments have shifted the balance of power from those who seek to protect their conversations and actions against surveillance to those who have access to the new devices. What was once Orwell's science fiction is now current engineering. In the field of psychological surveillance, the enormous expansion of polygraphing and personality testing into personnel selection in the 1950's has been matched by new technological developments such as covert polygraph measures, new truth drug research and the possibilities of reading emotional states currently opened by computer readings of brain-wave responses. Fears of manipulation and of penetration into the intimate spheres of autonomy through such techniques have made worried protests against "Big Brother" a growing response to such psychological surveillance.

The area which has undergone the greatest leap forward in technological capacity, however, is not physical or psychological surveillance, but data surveillance. The impact of data processing by computer is altering, in a way so profound that we are only barely aware of it as yet, the relation between individual spontaneity and social control in our society. As computers have made possible the collection, storage, manipulation, and use of billions of bits of information, at quite cheap prices and through operations done at incredible speeds, ours has become the greatest data-collecting society in human history. Government agencies, corporations, universities, churches, labor unions and a host of other organizations now collect many times the amount of information about their members, customers, or clients than they ever did before. More organizations exchange information from their files than ever took place before. More centralized records are growing up to collect information according to certain functional aspects of individual life—education records, employment records, military service records, medical records, security clearance records and many others. At the same time, the pressure to move from our present cash and check economy, with its relatively small-scale credit card sector, to a money-less transaction system, based on a computerized flow of credits and debits to central bank accounts for each individual (and fingerprint, voiceprint measures for unique identification) represents the most far-reaching utilization of computer capability, yet many experts in banking, government and corporate life state confidently that such an automated transaction system is on the way. Finally, as government has had to deal with its increased responsibilities in social welfare, law enforcement, civil rights compliance, economic regulation and forecasting, and national security, the pressures have mounted for centralized information systems that would apply large-scale data analysis on both a statistical and personal dossier basis.

Of course, the collection and storage in computers of vast amounts of personal data about individuals and private data about groups does not mean that we currently possess the technology to make all the comparisons, syntheses and retrievals that proponents of computer information systems sometimes claim or their critics sometimes envisage. A great deal of work is currently underway to make either the general data bank for statistical purposes or the "intelligence system" for specific enforcement yield up its capacity data in usable form. The more complicated the mix and match operations called for, the more difficulty this poses for the computer in its present form. Having made these points, however, it is important to note that these are probably temporary difficulties, virtually certain to be resolved in the coming decade.

This brief sketch of the interaction between technology, law and social values in American society during nearly two centuries, suggests in the briefest possible way the revolutionary character of the situation we are facing today. An enormous leap forward has been made in the power of public and private authorities to place individuals and private groups under close surveillance. In reaction, American society has stirred in alarm over the "Big Brother" prospects presented by these developments and

has mounted an energetic campaign to either outlaw or control the techniques that have outstepped classic legal and social restraints. This is the situation we find ourselves in in 1967. Among thoughtful segments of the American public and the law-making community, the search now is for a whole new framework for defining privacy in a technological age. A host of interventions, from statutes and judicial decisions to administrative rules and professional standards must somehow be devised to replace the current restraints which originated in and serviced an earlier period in our nation's history, but are outmoded today.

I am concerned here today with only one area of this problem—what I call data surveillance and the remainder of my remarks will be directed to this aspect of the problem. However, it is because this problem arises in the context of the technological advances in physical and psychological surveillance and public alarm over these threats to privacy, that the computer issue must be seen in a larger context.

In many ways American law is in the worst possible shape to deal with information processing and privacy, much worse than the task of modernizing its concepts in the fields of physical and psychological surveillance. In the physical and psychological areas, American law has clear cut concepts to build from—ideas such as trespass, intrusion, physical rights of property, etc.—but consider the difficulties of applying constitutional standards to the information process. First, American law has no clear cut definition of personal information as a precious commodity. It has well-developed notions of proprietary information, corporate records and similar business information, derived from medieval law on the secrets of trades and professions and codified in the American patent system. But when information is not needed to make a profit, when it involves the flow of disclosure about the individual among those he comes in contact with and those who exercise authority over him, American law has had no general theory of value, no set of rights and duties to apply as a general norm. Second, American law has had no general system for dealing with the flow of information which government agencies and other levels of government control, apart from a few examples such as census data (which has been closed to any additional circulation) and income tax (which has been given a set of additional areas of circulation controlled by statute or executive order). On the one hand, we have traditions of free circulation of information that arise in our credit investigation and public opinion collection processes. On the other hand, we have traditions of confidentiality and classified-secrecy which mark the other boundary. How information can circulate between these two poles and what to do with information systems that are likely to contain all of these types of information are problems that American law has not considered. Third, American law has not developed institutional procedures to protect against improper collection of information, storage of inadequate or false data, and intra-organizational use of such information for reaching decisions about individuals outside or inside the organization. Again, we have been most creative where tangible property rights have been involved. The Federal Administrative Procedure Act of 1946 assured businessmen facing federal regulatory agencies that they would know what information about them was going into the records in certain key types of government hearings, that they would have opportunities to present other information to challenge or modify this data, and that the record produced by such a procedure would be subject to review through higher administrative and judicial processes. The development of such a theory of information and government action was set back badly during the late 1940's and 1950's, when the loyalty-security problem produced large-scale information collection about individuals without open hearings which provided full due process. Without the opportunity to know what was in the record, to cross-examine those who had given the information, and to challenge the evaluation put on the information by government security officials, individuals were left without effective protection in their personal reputations and job rights. It is important to note that American law never came to a final resolution of this dilemma. Supreme Court decisions limited the scope of the loyalty-security process in government to truly sensitive agencies and trimmed back its application in various marginal areas such as the granting of passports. But it has never been held by the courts that an individual has a right to full due process in loyalty-security matters and thus one model for information challenge that still exists is a model which rejects the obligation of government to give individuals whose loyalty has been questioned the kinds of remedies that are available to businessmen when property rights are involved.

Finally, American law is seriously challenged by some of the technological aspects of computer information systems which tend to work against the kinds of reasonableness standards that the law tries to apply where balancing is necessary between privacy, disclosure and surveillance. If, for example, there were ways to assure that statistical data banks, such as the proposed Federal Data Center, could be set up so that they could not be transformed by those who run the system into a means of obtaining various sets of information about known individuals, American law could well set carefully differentiated standards for data banks and intelligence systems. But the clear message of the technological specialists involved is that identifying names or numbers must be left attached to statistical data if information from various sources is to be put together for statistical purposes and if longitudinal studies are to be made of specific individuals through time. When this is the case, American law must confront the possibility that data banks might become intelligence systems and it is this hard dilemma that is now deeply troubling the congressional committees and legal writers concerned with

the first wave of data-pool systems for federal and state governments.

This short summary of the ways in which American law is not well prepared for developing new doctrines to control mis-use of information collection does not mean that the future is gloomy. What it does mean is that the same kind of imaginative thinking and systematic programming and planning must be applied to this problem as went into the development of the technology for the information systems themselves. This is a job in which the most fruitful discussions can take place among the computer scientists, lawyers, social scientists and public officials. The sharing of expertise, the recognition of needs and values, and the setting of new balances are the key developments. To suggest the kind of approach that I think American society should take to information systems, let me sketch the response that I think sets these balances most sensitively. At the outset, I would have the courts and legislatures adopt as their guiding principle, the concept that an individual's right to limit the circulation of personal information about himself is a vital ingredient of his right to privacy and this should not be infringed without the showing of strong social need and the satisfaction of requirements for protective safeguards. The First Amendment to the American Constitution which guarantees our rights to freedom of speech, press and association must have as its necessary corollary the fact that we have a right not to communicate. It must also mean that we have the right to choose those to whom we communicate and the terms on which we do so. Any action by government that "turns us on" without that consent violates the right to silence that the Framers intended to give in the First Amendment just as much as the right to communicate. I would predict that this principle will come to be the guiding constitutional approach of the United States Supreme Court in dealing with the areas of physical, psychological and data surveillance. Following this approach, when government takes information from an individual for one purpose (such as income taxation, social security, government licensing and employment) and uses it to influence, regulate, or prosecute the individual on unrelated matters, this raises a question about violation of the confidence under which the information was originally given. The more that centralized information pools on individuals are assembled, the more serious the unrestricted flow of information becomes. This suggests that we need in our legal system some procedure for classifying information into various categories and distinguishing the rights to use of such information according to such classifications. For example, personal information could be divided into matters of public record that are expected to be open to virtually everyone; confidential information that is given in trust to certain individuals or agencies with the expectation of limited use; and security information which is either given under the expectation of complete non-circulation or which contains derogatory information about individuals that has been obtained by physical and psychological surveillance. Different standards must be set for the receipt, storage, and circulation of such different classes of information. This could be done by federal and state legislation, by administrative rules, and by the way in which information systems are technologically related to one another.

With these general proposals established, our policy-making would turn to the technological safeguards that could limit the capacities for mis-use of information systems. It is important to realize that storing data in computers rather than on pieces of paper in metal files allows us to create far more technological protection for sensitive information than in the era of written records and physical manipulation. For example, information "bits" in the memory banks could be locked so that only one or several persons who have special passwords could get to it. Computers could be programmed to reject requests for statistical data about "groups" which are really attempts to get information on specific individuals or organizations. A data system could be set up so that a permanent record was made of all inquiries and the "audit trail" could be subject to annual review by the management of the information center, independent "watch-dog" commissions of public officials and private citizens, and legislative committees.

Although many other ways to set system controls on information systems could be discussed, the fact remains that the system could still be "beaten" by those in charge of it, from the programmers who run it and the mechanics who repair breakdowns to those who are in charge of the enterprise and know all the passwords. This means that a network of legal controls is absolutely essential. For example, a federal statute could specify the data put into a statistical center is to be used solely for statistical purposes. It could forbid all other uses of the data to influence, regulate or prosecute anyone, making such use a crime, and excluding all such data from use as evidence in judicial or governmental proceedings. It could forbid all persons other than data center employees to have access to the files, and the data could be specifically exempted from subpoena. An Inspector General or Ombudsman-type official could be set up to hear complaints about alleged misuse, and judicial review for such complaints could be provided for.

A far more extensive set of safeguards are required when intelligence systems are involved. These must deal with which individuals go into the system at all, which public officials have access to the information, what classes of information are completely excluded and what safeguards are provided for challenging both the information collected and the use made of it. Regulations for mis-use of the information by the intelligence system personnel and by agencies which use the information would have to be provided and, again, some form of outside review of the system would be required, preferably by both an independent executive agency and legislative committees.

At the moment, American society is barely entering the beginning stage of this debate over data surveillance. We can see that three quite different approaches are already appearing. One position, reflected by the initial views of many newspaper editors, civil liberties groups and congressional spokesmen is to oppose creation of data centers and intelligence systems completely. The need for better statistics for policy analysis or of richer information systems for criminal justice purposes is seen as inadequate when weighed against the increase in government power and fears of invasion of privacy that such systems might bring.

A second view, reflected in the initial thinking of many executive agency officials and computer scientists assumes that traditional administrative and legal safeguards, plus the expected self-restraint of those who would manage such systems is enough to protect the citizen's privacy. The more reflective spokesmen in this group would add that a large-scale decrease in the kind of personal privacy we have through inefficiency of information collection may well be on its way out, but that this would be something individuals could adjust to and would not seriously threaten the operations of a democratic society.

The third position, which I have tried to describe in my earlier discussion, assumes that neither the "total ban" nor the "traditional restraints" positions represent desirable alternatives. What is called for is a new legal approach to the processing of personal information by authorities in a free society and a new set of legal, administrative, and system protections to accomplish this objective. The fact is that American society wants both better information analysis *and* privacy. Ever since the Constitution was written, our efforts to have both order and liberty have succeeded because we found ways to grant authority to government but to tie it down with the clear standards, operating procedures and review mechanisms that protected individual rights. A free society should not have to choose between more rational use of authority and personal privacy if our talents for democratic government are brought to bear on the task. The most precious commodity we have now is the few years of lead-time before this problem grows beyond our capacity for control. If we act now, and act wisely, we can balance the conflicting demands in the area of data surveillance in this same tradition of democratic, rational solutions.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21 - 24

1970

ROLE OF PROFESSIONAL SOCIETIES IN ESTABLISHING ETHICAL GUIDELINES

By

Mr. Mens Kutt

PRESIDENT OF CANADIAN INFORMATION PROCESSING SOCIETY

PRESIDENT OF CONSOLIDATED COMPUTER SERVICES LTD.

ROLE OF PROFESSIONAL SOCIETIES IN ESTABLISHING ETHICAL GUIDELINES

ABSTRACT

A representative group of senior members of the Canadian Information Processing Society (CIPS) believes that advances in information handling technology should not be lost because adequate safeguards to protect the individual can be devised.

We believe our role in establishing safeguards for the individual's right to privacy should be as follows:

a) Together with other computer societies implement professional standards and a code of ethics for members involved in data handling activities.

b) Educate our members in the sensitivity of the problem of protecting individual rights through conferences and publications.

c) Assist the Government in the drafting of legislation to ensure among other things that the individual has access and recourse concerning information filed on him.

The approach to the privacy-data bank problem must be multi-pronged with computer societies, representing users and companies in the industry, and the Government working together to ameliorate the serious situation that could develop in the future as man begins to utilize the information handling technology presently at his disposal.

ROLE OF PROFESSIONAL SOCIETIES IN ESTABLISHING ETHICAL GUIDELINES

Members of the Canadian Information Processing Society (CIPS) see the privacy-data bank question as representing a spectrum of problems. The spectrum ranges from the innocent misuse of files such as mailing lists, to damage to the individual caused by inaccurate or incomplete information filed on him, and on the extreme side, to flagrant blackmail.

Before considering corrective action let us look at some other dimensions of the problem. We've always had a privacy problem. We always will have one as long as we wish to take advantage of modern conveniences such as a credit rating.

The dilemna we face is that on the one hand we have the opportunity to tremendously improve the lot of the individual with the computer's information handling capabilities but on the other, we could do considerable harm to the individual if this information is misused. For example a national medical data bank would benefit all Canadians but what would happen if someone tried to blackmail individuals with histories of mental disorders?

Another dimension of the privacy-data bank question is that it does not present a serious problem today because man has

only just begun to effectively utilize the information handling technology at his disposal. The rapid expansion of time sharing, with the use of many remote terminals to a large data base, represents the catalyst that could make the problem an extremely serious one.

Members of CIPS believe that the benefits to the individual of advances made in information handling technology should not be lost. Adequate safeguards to protect the individual can be implemented. However the time to implement the safeguards is now, before data banks begin an uncontrolled growth.

What can these safeguards be? First of all the problem is people oriented rather than technical oriented. By this I mean that there is very little that can be done from the technical point of view that computer operational people, if they choose, cannot undo. This is not to say that systems design should not incorporate features for protection against the inexperienced user. What I do say is that if people understand the system, and decide to misuse it, very little can be done to stop them.

With the people dimensions of the problem, computer societies can play a significant role in preventing a

serious situation from occuring. 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. This could be accomplished through conferences and publications. The second thing societies should do is establish professional standards and a code of ethics for computer people involved in information handling activities. This latter factor will require considerable co-operation between the computer societies.

These two factors represent the practical extent to which computer societies, representing users and industry, can be self-policing. They will not by themselves be adequate to protect the rights of the individual. Government involvement and legislation will be necessary and this represents the third major area in which computer societies have the technical knowledge that will be necessary to draft effective legislation and should assist the Government. Careful attention must be given to all dimensions of the problem to avoid precipitous action. The legislation should ensure that the individual has the opportunity to check the contents of his file and also that he has the right to approve the transfer of this information to other files. In this way the individual's right to privacy can be protected.

In summary, advances in information handling technology offers us tremendous possibilities for the future which should not be lost. We can protect the rights of the individual with a multi-pronged approach:

Computer societies should:

1) Establish a code of ethics for people dealing in sensitive information.

2) Educate their members on the rights of the individual.

Government should:

3) Legislate to ensure the individual has access and recourse concerning the information filed on him.

May 19, 1970.
/gl

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER

Le droit à la vie privée dans le monde moderne

by Pierre Juvigny

Paper presented at a UNESCO Meeting, Paris, January 19-23, 1970

DOCUMENT

Le droit à la vie privée dans le monde moderne

par Pierre Juvigny

Communication présentée à la réunion d'experts de l'UNESCO sur le droit à la vie privée

Paris, 19-23 janvier 1970

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

SHC/CONF.12/10
PARIS, le 14 janvier 1970
Original : français

ORGANISATION DES NATIONS UNIES
POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

REUNION D'EXPERTS SUR LE DROIT A LA VIE PRIVEE

Paris, 19 - 23 janvier 1970

LE DROIT A LA VIE PRIVEE DANS LE MONDE MODERNE

par

PIERRE JUVIGNY

Les opinions exprimées dans ce document n'engagent que leur auteur

I. INTRODUCTION

Le respect de la vie privée de l'individu et de sa famille peut être contesté dans son principe même ; certaines sociétés, fondées sur le clan, la tribu, ont ignoré le concept de vie privée et, a fortiori, les droits et garanties qu'implique un tel concept. Les impératifs de la vie, voire de la survie, dans une nature hostile sont alors tels que le groupe ne peut dominer la nature ou composer avec elle que grâce à une vigilance de tous les instants, à une mobilisation permanente de toutes les forces disponibles, ce qui implique une organisation "sociale" hiérarchisée, où l'homme et sa famille sont subordonnés aux objectifs d'un groupe plus large, définis par des voies parfois autoritaires, parfois "démocratiques" (conseils des anciens, des sages, des chefs de tribus, etc.), mais qui laisse peu de place à des droits subjectifs (au sens juridique du terme) de l'individu contre le clan ou la société.

Pourtant, la notion de respect de la vie privée n'est pas l'apanage de la philosophie des droits de l'homme telle qu'elle a été définie en Occident au cours des trois derniers siècles. Souvent, la tradition religieuse reconnaît des droits à la famille (voir notamment Unesco "Le droit d'être un homme" et Séminaire d'Oxford,) - "Vivre à sa guise" (mais dans le respect des lois), imprègne la civilisation grecque, et Antigone n'exprime pas seulement des rapports de nature politique mais traduit la revendication d'une autonomie individuelle d'où dérive nécessairement "la vie privée" sans laquelle l'opposition individu-société ne serait même pas concevable.

A travers l'histoire, on pourrait relever les moments nombreux où affleure, puis s'épanouit - dans des civilisations pourtant fort différentes - la notion de liberté individuelle - y compris le respect de la vie privée - ; mais, en d'autres moments, ces dernières notions s'effacent au profit de tendances absolutistes visant à "intégrer" l'homme dans une société qui, même si elle ne dénie pas, en théorie, tout droit à l'individu, ne peut tolérer qu'il en use largement.

Dans le monde moderne, "le respect de la vie privée" n'est pas une notion universellement admise. Entre les deux dernières guerres, les Etats totalitaires, parce que totalitaires, ne pouvaient reconnaître, ni garantir, à moins d'être en contradiction avec leur philosophie et leur finalité - "le droit à la vie privée, exempt d'immixtions arbitraires, ..."

Plus récemment - et ce n'est qu'un exemple - on peut raisonnablement s'interroger sur le sens du respect de la vie privée dans le régime chinois qui, périodiquement, mobilise les masses au service de fins absolument collectives et dans des conditions qui excluent, semble-t-il par nature même, la notion de "vie privée".

Quoi qu'il en soit, la Déclaration universelle des droits de l'homme, puis le Pacte des Nations Unies, relatifs aux morts civils et politiques - et d'autres instruments élaborés par des institutions de la famille des Nations Unies et par des organisations régionales consacrent tantôt explicitement, tantôt de façon dérivée ou indirecte, le concept de respect de la vie privée. Et dans la mesure où les normes sont inscrites dans les Actes des institutions internationales et dans de nombreux instruments, on doit les admettre comme éléments du patrimoine commun de l'humanité (voir Résolutions de la Conférence de Téhéran), et comme principes de la société internationale.

II. ASPECTS PERMANENTS DU DROIT AU RESPECT A LA VIE PRIVEE ET ASPECTS INHERENTS A SA MISE EN OEUVRE ET A SA PROTECTION DANS LE MONDE MODERNE

A. Introduction

Les conditions dans lesquelles le droit au respect de la vie privée est reconnu et protégé a donné lieu depuis des siècles à de nombreuses solutions constitutionnelles, législatives, réglementaires et aussi à des pratiques et usages reconnus, appliqués et sanctionnés par les tribunaux.

Les problèmes posés par la mise en oeuvre de l'article 12 de la Déclaration universelle des droits de l'homme ne sont pas d'une nature nouvelle. Il s'agit, aujourd'hui comme hier, de tracer les limites de la vie privée et des pouvoirs de l'Etat et de ses organes, d'instituer des garanties de tous ordres pour assurer la protection effective de ce droit tant contre les immixtions arbitraires du pouvoir exécutif et de l'administration que contre les atteintes que pourraient commettre des individus ou des groupes.

La vie en société implique nécessairement (et impliquera toujours) des limitations à la vie privée. Elle suppose, au minimum, la connaissance par l'Etat ou, plus généralement, par les "pouvoirs publics" de certaines données qui, stricto sensu, peuvent (ou pourraient) relever, selon une interprétation large, de la "vie privée" : Il n'y a pas de société viable sans Etat civil, sans livrets scolaires, sans conscription, sans archives, sans statistiques, sans dossier fiscal, sans casier judiciaire, etc. Les institutions et les procédures légitimes que les nécessités sociales ont, en quelque sorte, secrétées sont inhérentes à l'organisation sociale.

Sur un autre plan, parce que les rapports au sein de la société ne sont pas exclusivement ceux de "l'individu et du Pouvoir" (Alain), des garanties et des

protections ont été prévues en faveur de l'individu contre les violations indues à la "vie privée" commises par d'autres individus ou par des groupes distincts de l'Etat.

Mais, la nouvelle révolution scientifique et technologique pose des problèmes parfois inédits ou, au moins, confère à des problèmes anciens certains aspects nouveaux.

B. Problèmes et aspects nouveaux de la protection de la vie privée dans le monde moderne

L'étude des aspects nouveaux de la protection juridique de "vie privée" doit être conduite en relation étroite avec l'analyse des moyens nouveaux qui rendent possibles, dans le monde moderne, des atteintes accrues à la vie privée.

Il convient, dans les recherches que peut faire notre colloque, d'exclure l'attitude a priori hostile aux progrès scientifiques dont découlent des menaces nouvelles. L'emploi du terme menace est déjà un jugement de valeur!

L'attitude efficace consiste à analyser la nature, la puissance et les aspects nouveaux des moyens modernes et à rechercher la conciliation de ces moyens avec le respect de la vie privée, c'est-à-dire, là encore, à tracer des normes, des limites et des procédures de garantie de la vie privée adaptées à la nature même de ces moyens.

Cette recherche ne peut d'ailleurs exclure la prise en considération de certains droits proclamés dans la Déclaration universelle des droits de l'homme et qui, tout aussi respectables que les droits énoncés dans l'article 12, peuvent entrer en conflit avec ces derniers.

1. Accroissement des moyens de connaissance de "la vie privée"

(a) Techniques d'enregistrement

L'élément caractéristique des diverses techniques modernes d'enregistrement est la clandestinité. Qu'il s'agisse du téléobjectif, des écoutes et des espions téléphoniques, des verres polaroïdes/1 et peut-être, demain, d'éléments miniaturisés qui permettraient de contrôler, voire de télécommander le comportement d'un individu à tout moment, et à son insu ...

L'utilisation de ces divers moyens par les pouvoirs publics pose de nombreux problèmes juridiques.

Même si dans beaucoup de pays les cours et tribunaux ont tendance à rejeter les renseignements ainsi obtenus comme éléments de preuve - et ce, d'autant plus que la falsification de l'enregistrement authentique n'est pas exclue -, il reste que la licéité de tels enregistrements et de leur utilisation sur le plan juridique devrait faire d'abord l'objet d'études.

---

1. Joseph W. Bishop Privacy vs. Protection.
The Bugged Society et Assemblée pour les droits de l'homme, Montréal, 22-27 mars 1968.

Le danger apparaît, en tout état de cause, lorsque l'utilisation de tels procédés est le fait d'organes de l'Etat qui échappent largement aux contrôles - parlementaires, juridictionnels, administratifs ou autres - auxquels sont normalement soumis les services publics traditionnels. Dans un monde où s'épanouissent des structures parallèles, officieuses, voire clandestines dans les domaines de la police, du renseignement et de la surveillance ..., il est évident que l'utilisation par ces services de tels enregistrements peut constituer une arme de pression et de chantage de nature à affecter le fonctionnement de toute société démocratique, sur le plan législatif, exécutif et judiciaire.

Les dangers ne proviennent pas seulement des organes de l'Etat.

La popularisation de ces moyens d'enregistrement rend possible l'espionnage privé dans des conditions qui sont sans commune mesure avec les techniques artisanales utilisées en d'autres temps par les maris jaloux, les commères et les concierges indiscrètes. Les atteintes peuvent avoir lieu dans l'immeuble où la famille réside. Elles peuvent être aussi le fait d'un membre de la famille contre un autre membre de la famille (en vue d'une instance en divorce, par exemple). Enfin, l'espionnage privé peut, sur le plan commercial, technique, financier, s'exercer entre sociétés concurrentes mais aussi à l'intérieur de l'entreprise (par exemple : enregistrement clandestin des conversations des chefs de service par le président ou le directeur général de la firme) ; dans de tels cas, même lorsqu'il ne s'agit pas de "vie privée", il s'agit de rapports de droit privé.

Les entreprises dont la fonction est d'informer peuvent céder d'autant plus aisément aux immenses possibilités qu'offrent les techniques clandestines d'enregistrement qu'elles sont accoutumées de longue date à l'utilisation de toutes les techniques audio-visuelles.

Le respect de la vie privée et le droit à l'information (et plus généralement tous les droits à l'expression ou à la communication des faits et des idées ... reconnus par la Déclaration universelle) peuvent ici entrer en conflit. Là encore le problème de l'utilisation licite et de l'utilisation indue, illicite, illégale, prohibée se pose en des termes relativement nouveaux, dans la presse, la radio, la télévision.

2. Informatique, recueil et centralisation des informations

Les possibilités d'utilisation des ordinateurs dans les services publics exercent sur les responsables des services d'"Organisation et méthodes" une compréhensible fascination. Qu'il s'agisse de la collection des renseignements, de leur interprétation, de la programmation, de la préparation des décisions ("decision making"), de l'amélioration des services de l'Etat civil, de la conscription, du casier judiciaire, de la gestion des administrations fiscales, du personnel, des matériels et des stocks, etc., de la planification globale et sectorielle, l'emploi des ordinateurs paraît tout à la fois permettre une gestion économique des services publics et l'accroissement de leurs moyens d'action et de l'efficacité de leurs programmes.

L'introduction de l'"informatique" dans les divers services publics pose de multiples problèmes dont certains peuvent indirectement affecter la "vie privée". On se limitera ici aux problèmes qui paraissent relever directement du droit à la vie privée.

Les dangers que l'on peut immédiatement identifier ont trait aux aspects de la "vie privée" qui sont actuellement couverts, dans de nombreux pays, par un faisceau législatif de "secrets professionnels" définis en termes précis. La centralisation dans un "overall computer" (ordinateur universel) de tous les renseignements concernant un individu depuis sa naissance et dans tous les aspects de son existence (scolaire, militaire, médical, professionnel, fiscal, pénal, etc.) donnerait à ceux qui auraient accès à cet instrument un pouvoir considérable d'influence et de pression. En d'autres termes, l'insertion - inévitable - de l'informatique dans les services publics ne saurait être opérée sans une prise de conscience des problèmes qu'elle peut poser du point de vue du respect de la "vie privée" et sans l'examen des procédures juridiques qui pourraient être adoptées pour établir un équilibre entre les indéniables améliorations que l'utilisation de l'informatique peut apporter aux services publics et le respect de la vie privée. En tout cas, si l'on insérait dans les fiches qu'alimentent les machines des informations obtenues par les moyens clandestins et illicites (mais tolérées) auxquels il a été fait ci-dessus allusion, les dangers d'atteinte à la vie privée seraient alors considérables.

Un autre danger de l'utilisation de l'informatique tient au fait qu'elle accroit le risque technocratique. Dès lors que l'on s'en remet à la machine pour "rationaliser" les choix budgétaires, trancher les options en matière de planification et de "Développement" de politique militaire, d'aménagement du territoire, de politique scolaire, etc., - avec ce que cela comporte de "rigidité", les choix étant opérés par la machine" - la notion de démocratie peut être remise en cause ; les choix opérés mathématiquement excluent, en effet, - du moins a priori -, les éléments psychologiques collectifs ; même si on les insère accessoirement dans les données sur lesquelles travaille l'ordinateur, elles ne peuvent qu'avoir une importance secondaire.

Dans ce contexte, l'atteinte à la vie privée n'est certes pas directe. Mais la technocratie disposant des ordinateurs peut accéder à une puissance telle que la vie privée sera restreinte à un domaine étroit et que la vie de l'individu et de sa famille sera conditionnée par les ordinateurs dès qu'elle pourrait avoir une incidence quelconque dans le domaine économique et social.

3. Progrès de la médecine et d'autres sciences et techniques

Les rapports entre les différents droits qui régissent les rapports entre l'individu, la médecine (et les services sociaux) et plus généralement les autres sciences et techniques ne sont pas aisés à définir.

L'article 12 de la Déclaration universelle des droits de l'homme proclame le Droit à la vie privée. L'article 5 prohibe ... "les traitements cruels, inhumains ou dégradants". L'article 22 reconnaît le droit à la Sécurité sociale, l'article 25 le droit de tout individu à un niveau de vie suffisant pour assurer sa santé, son bien-être et ceux de sa famille ..., à la sécurité en cas de chomage, de maladie, d'invalidité, de veuvage, de vieillesse ou, dans les autres cas, de perte de ses moyens de subsistance par suite de circonstances indépendantes de sa volonté".

La vie "médicale" de l'individu a été, dans certains pays et pendant des siècles, considérée comme l'un des éléments de sa "vie privée". Cependant, la médecine sociale et la Sécurité sociale ne peuvent être mises en oeuvre sans que

l'appareil administratif impose à l'individu, seul ou chef de famille, des "déclarations" sur son état de santé et ses variations ; la couverture, par des institutions sociales, des risques (maladie, maternité, invalidité, etc.) conduit nécessairement à l'institution d'organismes qui sont chargés de payer et doivent donc tout naturellement prévenir les abus, contrôler la réalité de la maladie, lutter contre les interprétations trop libérales des médecins, etc.

L'institution de toute médecine sociale généralisée pose de délicats problèmes qui touchent nécessairement à la "vie privée" et qui ne peuvent être résolus par le seul recours aux normes qui prévalaient à l'époque où la médecine était intégralement libérale.

Si ces problèmes sont nés, notamment, avec la généralisation de la Sécurité sociale, les progrès récents de la médecine et de l'informatique leur confèrent depuis peu une indéniable acuité./[1] (Le sujet du colloque étant limité à la "vie privée", les nécessités et les formes de la protection de l'intégrité de la personne physique, morale et intellectuelle en fonction des progrès de la biologie, de la médecine et de la biochimie ne sont pas traitées dans la présente communication - on les examinera, le cas échéant, de façon marginale au cours du colloque)

Enquêtes; sondages, tests

La prolifération des enquêtes et sondages tendant à dégager les attitudes et tendances de l'opinion ou de groupes pose, elle aussi, des problèmes auxquels les législateurs n'ont porté jusqu'à présent qu'une faible attention. Tandis que les renseignements recueillis par les services publics sont soumis à des règles strictes sur le secret professionnel, - souvent fort détaillées -, ceux recueillis par les entreprises privées de sondage ne sont pas, en général, soumis à des règles législatives assorties de dispositions répressives. Les nécessités techniques des sondages politiques, sociaux, économiques conduisent à poser des questions auxquelles les "enquêtés" répondent spontanément sans mesurer le degré d'intrusion dans leur vie privée que représentent ces enquêtes et les risques d'utilisation indue de ces renseignements.

Les questionnaires que doit remplir le candidat à un prêt vont très souvent au-delà des seuls éléments destinés à garantir la solvabilité de l'emprunteur. Quant aux questionnaires et tests au moment de l'embauchage des travailleurs, leur contenu constitue fréquemment une intrusion dans la vie privée qui n'est pas strictement dictée par les seules exigences de la mesure de la capacité professionnelle (questions portant sur la religion, les opinions politiques, les habitudes alimentaires, la vie conjugale, les lectures, etc.).

III. MESURES DE PROTECTION DE LA VIE PRIVEE

Quelques Etats, des ONG, les Nations Unies (voir résolution 2450 (XXIII) de l'Assemblée générale - 19 décembre 1968), les institutions spécialisées, les institutions régionales (notamment le Conseil de l'Europe) se préoccupent des

1. En vue de ne pas charger excessivement la présente communication, l'auteur s'est abstenu de développer ce point. Il donnera, si nécessaire, des exemples concrets lors du colloque.

rapports entre les progrès de la science et de la technologie et des droits de l'homme (y compris le droit au respect de la vie privée).

Deux observations doivent être formulées au présent stade :

1. On n'est pas parvenu, jusqu'à présent, à formuler des règles claires et efficaces pour résoudre ces problèmes. La complexité de la matière et aussi le fait que telle règle juridique formulée en termes trop précis risquerait d'être rapidement inadaptée, tant est rapide l'évolution scientifique et technique, expliquent la relative lenteur des travaux et la prudence des autorités publiques. Toutefois, il est réconfortant de constater que ces problèmes font l'objet d'études et de relever que certaines recommandations sont déjà soumises aux instances gouvernementales dans plusieurs pays.

2. Ces problèmes ne relèvent pas de la seule compétence technique de spécialistes ; ils sont interdisciplinaires. L'analyse des conséquences de l'informatique sur les Droits de l'homme ne peut être faite que grâce à la collaboration des spécialistes de cette technique, des juristes, des administrateurs, etc. Cette méthode est valable mutatis mutandis lorsqu'il s'agit des conséquences des progrès de la médecine, de l'information, etc.

D'ores et déjà, on peut noter ici quelques tendances qui commencent à se dégager de ces travaux ; on peut aussi mentionner les méthodes - principalement juridiques - qui pourraient être utilisées en vue d'assurer la protection du "droit à la vie privée" dans le monde moderne.

S'agissant de problèmes qui touchent aux droits civils et politiques, c'est, dans la plupart des systèmes constitutionnels, le législateur qui est compétent pour modifier les lois existantes. Lorsque le droit existant ne "couvre" pas les utilisations abusives des découvertes nées de la science et de la technologie modernes, la promulgation de lois nouvelles s'impose.

Dans certains cas, la tâche peut sembler aisée : mesures préventives telle que l'interdiction de la fabrication ou de la vente des espions téléphoniques, mesures assorties de peines en cas d'infraction ; énumération limitative des personnes publiques et des professionnels autorisés à utiliser certains instruments (notamment d'enregistrement) ou certains procédés ; réglementation de leur condition d'utilisation. Mais les mesures d'interdiction pure et simple seraient souvent illégitimes.

Par exemple, interdire l'utilisation des téléobjectifs aurait pour effet de priver certaines activités professionnelles d'un instrument utile. Ce sera donc, le plus souvent, l'interdiction de l'utilisation attentatoire aux Droits de l'homme et notamment au droit au respect de la vie privée et la répression de ces utilisations indues qui devra être adoptée.

C'est le caractère clandestin qui peut constituer le critère juridique de l'interdiction et des sanctions ; l'enregistrement clandestin (à le supposer licite) ne devrait en aucun cas être utilisé sans l'autorisation expresse de l'intéressé.

En outre, tout un faisceau complémentaire de sanctions pourrait être utilisé (droit de rectification en cas d'utilisation des documents par la presse et les détenteurs des moyens audio-visuels d'information, action en réparation largement ouverte à la victime des pratiques dommageables, etc.).

Dans certains domaines, l'utilisation des procédés modernes devrait être placée essentiellement sous le contrôle de l'autorité judiciaire (notamment les écoutes téléphoniques).

Mais l'action du législateur et du pouvoir judiciaire ne saurait suffire. En particulier, la conciliation entre la liberté de l'information et le respect de la vie privée exclut des mesures législatives qui aboutiraient à une véritable censure s'abritant derrière les nécessités de la mise en oeuvre effective du droit au respect de la vie privée, ou à une "fonctionarisation" des journalistes. C'est donc aussi par l'adoption, par les professionnels, de code de déontologie que les abus pourraient être prévenus, en tout cas limités, voire réprimés.

Dans beaucoup de pays, la nécessité d'une législation entièrement nouvelle apparaît en ce qui concerne les tests, les sondages, etc.. L'institution de "secrets professionnels" définis par la loi en termes rigoureux, la prohibition de "questions" contraires aux principes de la Déclaration universelle (religion, convictions politiques, éléments de la vie privée, etc.) pourraient, entre autres mesures, combler les lacunes actuelles des codes.

L'utilisation de l'informatique par les services publics dans les conditions qui ont été exposées ci-dessus et les risques qu'elle comporte pour la vie privée devraient conduire à la mise en oeuvre de garanties nouvelles. L'énumération des personnes qui auront accès aux différents ordinateurs où sont stockés les renseignements - et a fortiori, à l'ordinateur central - devrait figurer dans des textes législatifs ou réglementaires et les obligations du secret professionnel devraient être renforcées. En outre, pour éviter l'accumulation de renseignements portant sur la vie privée et obtenus dans des conditions clandestines, le droit de toute personne à la "communication de son dossier" devrait être reconnu.

On peut se demander si, en sus des dispositions législatives ou administratives, l'institution d'un contrôle effectué par "un collège de sages", inspiré de l'"ombuds man", ne contribuerait pas à prévenir les tentations d'utilisation, par certains services, de l'informatique à des fins étrangères à l'intérêt général.

Il est évident que de telles mesures (qui ne sont qu'indicatives) ne seront vraiment efficaces que si l'éducation des hommes d'aujourd'hui et de demain réserve une large place aux valeurs permanentes - proclamées dans la Déclaration des droits de l'homme.

Sinon, l'utilisation des immenses moyens scientifiques et techniques modernes, qui pourrait être l'instrument de la libération de l'homme, conduira à son aliénation inconsciente ou consciente, voire recherchée.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER

Human Rights and Scientific and Technological Developments

Report of the Secretary General

United Nations Economic and Social Council-Commission on Human Rights

DOCUMENT

Les droits de l'homme et les développements scientifiques et technologiques

Rapport du Secrétaire général

Conseil économique et social des Nations unies - Commission des droits de l'homme

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

UNITED NATIONS

ECONOMIC
AND
SOCIAL COUNCIL

Distr.
GENERAL

E/CN.4/1028/Add.3
4 March 1970
ENGLISH
ORIGINAL: ENGLISH/FRENCH

COMMISSION ON HUMAN RIGHTS
Twenty-sixth session
Item 18 of the provisional agenda

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Report of the Secretary-General (continued)

III. USES OF ELECTRONICS WHICH MAY AFFECT THE RIGHTS OF THE PERSON AND THE LIMITS WHICH SHOULD BE PLACED ON SUCH USES IN A DEMOCRATIC SOCIETY

1. Problems affecting human rights

274. Various electronic devices have been referred to in chapter I. In this chapter, attention is given mainly to electronic data banks, to electronic automation and to electronic communications media.

A. Electronic data banks

275. The following classification of the kinds of data banks currently in operation has been suggested by Westin:

> "(T)he intelligence /data bank/ system is one in which decisions affecting the civil rights of the citizen as an individual will be made as a result of information supplied by the data bank. Examples would be the criminal justice information systems... that accumulate data for purposes of law enforcement, or personnel security, and loyalty data banks as these may develop... to collect information for purposes of personnel screening. The characteristic of such systems is that the files are organized according to each individual entered into the system, and the primary use of the files is to judge that individual in ways that would have a direct effect upon his civil rights.
>
> "Regulatory data banks in the governmental sector are those that are developing to deal with the economic, social, and welfare aspects of the citizen's life, and would encompass government systems of data banks in the fields of education, welfare, health, business regulation, and the like. The data may be grouped according to classes of people but often the files are on an individual basis, and will be a major determinant of whether benefits and favours supplied or regulated by government are available to a particular individual or the group or class to which he belongs.
>
> "Statistical data banks in government are bodies of data collected in order to evaluate the operations of government agencies themselves or to provide data about developments in society on a statistical basis upon which to base government policies and responses." 210/

210/ Alan F. Westin, "Discussion Memorandum on Legal Aspects of Privacy in Computer Data Banks" (October 1968), p. 4, a paper prepared for the Privacy Committee of the American Civil Liberties Union.

276. Such data bank systems as these are increasingly used by Governments and in private enterprises and institutions. For instance, they play roles in relation to law enforcement, social security and health protection, census statistics, medical diagnosis, banking, credit rating, travel reservations and social research. The human rights problems which arise from this development may be examined primarily in relation to: (a) the accuracy of the information stores; (b) the question of who has access to the information; and (c) the question whether information could not be stored in a fashion which would protect the privacy of the individual.

277. It has been said that there are three basic ways in which inaccurate information on an individual may be recorded in a computed:

> "(a) The input data may be wrong, either because an error was made in recording it, or because it has been wrongly transcribed. With incorrect data even perfect processing must give an incorrect result...
>
> "(b) The computer's programme may be wrong, for example, because the programmer did not appreciate the full circumstances of the case, or because he made a logical mistake through faulty analysis, or because of copying or transcription errors in writing the programme down and preparing it for feeding into the computer.
>
> "(c) The computer develops a mechanical or electrical fault which causes it to corrupt the date, the programme or the results." 211/

278. Once in a file, information, however inaccurate, tends to remain there, and the nature of the computer strengthens this tendency, first because of the difficulty of finding out errors among the mass of information that can be handled by a computer, and secondly because of the relative ease and economy of retaining the entire information gathered, as compared with an ordinary filing system. 212/

211/ Joseph Jacob in (United Kingdom) National Council for Civil Liberties, NCCL News Release (26 June 1969), quoting from F.J.M. Laver, Introducing Computers (London, 1965).

212/ Jack Sawyer and Howard Schechter, "Computers, Privacy, and the National Data Center: the Responsibility of Social Scientists", American Psychologist, vol. 23, No. 11 (November 1968), p. 815.

279. Individuals are vulnerable to the danger that subjective data, that is to say, evaluations based for instance on interviews, are recorded in a computer and later treated as objective facts.213/ This danger varies according to the quality of the source of information and of the personnel interpreting the computer's output.

280. Secondly, erroneous information can result from a data-processing system as a consequence of faulty programming. Mistakes may enter the process between the preparation of a programme and its installation as a set of instructions for the computer; but a more serious potential source of errors and distortions at this stage is the programmer himself. As Professor Arthur R. Miller, of the University of Michigan, has put it:

> "Our success or failure in life ultimately may turn on what other people decide to put into our files and on the programmer's ability, or inability, to evaluate, process, and interrelate information. The great bulk of the information likely to find its way into the /proposed data bank/ center will be gathered and processed by relatively unskilled and unimaginative people who lack discrimination and sensitivity." 214/.

281. Finally, erroneous information can result from a mechanical or electrical fault in the computer. The developing technique of time-sharing may present further possibilities for accidental malfunction. Professor Donald N. Michael, Program Director of the Center for Research on Utilization of Scientific Knowledge at the University of Michigan, has written:

> "This /time-sharing/ means that while one user's finger is moving toward a control button on his computer control panel, another person is using the circuits he will be using a few seconds later. In the future, one computer user might accidently gain access, through equipment malfunction, to another's information stored in memory banks." 215/

213/ Ibid., p. 814.

214/ Arthur R. Miller, "The National Data Center and Personal Privacy", The Atlantic (November 1967), p. 54.

215/ Donald N. Michael, "Speculations on the Relation of the Computer to Individual Freedom and the Right of Privacy", George Washington Law Review, vol. 33, No. 1 (October 1964), p. 270.

282. It may be felt that the Assembly for Human Rights which met in Montreal, 22-27 March 1968, had the question of accuracy in mind when it stated that "non-governmental organizations of the legal profession should apprise themselves of the risk of computerized dossiers...".216/

285. Centralization in a computer memory of information previously retained in numerous scattered files in a traditional filing system presents problems of controlling access to so much information located in one place about an individual. A dual aspect of this kind of centralization has been described by Professor Michael:

> "/C/entralization of private information and its preservation in computer memories may decrease illegitimate leaks of that information. Those who will have access to personal history will see much more of it than was usually the case when it was contained in printed records, but fewer curious eyes will have knowledge of any part of the private history of the individual." 217/

284. Writers have drawn attention to the danger to the individual of allowing a governmental authority to have access to such a mass of information about him as can be contained in a computer, if such information is collected from all the official agencies which already have such data.218/ It has been claimed:

216/ Montreal Statement of the Assembly for Human Rights (Montreal, 1968), sect. IX.

217/ Michael, loc. cit., p. 270.

218/ Quite apart from the computer, the expansion of information gathering and record keeping in most societies has been considerable in recent years. Professor Westin (Privacy and Freedom, p. 161), has described this development as follows:

> "To help himself, to help science, and to help society run efficiently, the individual now pours a constantly flowing stream of information about himself into the record files - birth and marriage records, public-school records, census data, military records, passport data, government and private employment records, public-health records, civil-defense records, loyalty-security clearance records, income-tax returns, social-security returns, land and housing records, insurance records, bank records, business reporting forms togovernment, licensing applications, financial declarations required by law, charitable contributions, credit applications and records, automobile registration records, post-office records, telephone records, psychological and psychiatric records, scholarship or research-grant records, church records - and on and on. New forms of financial operations have produced the credit card, which records the where, when, and how-much of many once-unrecorded purchasing, travel and entertainment transactions of the individual's life. Through miniaturization, previous physical limits on such data storage have been overcome...
>
> "Second, the mobility of persons and the standardization of life in mass society have led to the development of large private and governmental investigative systems."

> "[Even] authorized use by the Government itself of this mass of data raises the specter of a government which knows all or which, having found that it does not know enough, devises further methods of obtaining the portion of the data which is still missing. One of the important features of a democratic government is the doctrine of the separation of powers which makes it difficult for any branch of the government to jeopardize the fundamental rights of the individuals. Certainly, at present, the multiplicity of agencies and procedures and the resulting red tape protect the individual against undue invasion of his privacy by making it more difficult for various government officials to know enough to cause real trouble. But if all the available data are integrated and stored in a computer in a way permitting instantaneous access to the record of each person, a sword of Damocles is going to hang all the time over the head of everybody." 219/

Similarly, it has been said:

> "Individually, and in the proper hands, each piece of information would be harmless enough, but out of context and in conjunction with dissimilar information it could be damaging." 220/

285. Attention must also be drawn to the position of the programmer, which gives him a key role in relation to the issue of privacy, as described by Professor Michael:

> "No one using the output from a computer needs to know as much about the data fed into it as does the programmer. Without intimate and extensive understanding of the data and the uses to be made of it, the programs which determine how the computer operates, and hence the quality of its output, will be crude. On the other hand, executive decisions often depend less on knowledge of details than on overall grasp of the situation. As a result, the programmer often will be the person with potentially the most intimate knowledge of the private lives of those whose data is processed. This potentiality need not result in his having specific knowledge about specific people, since a programmer is unlikely ever to see the materials which are input to the computer whose processes he has arranged. But given his deeper understanding of how the data are being processed, what assumptions are made about the relationships among the data, what constraints must be put on the data in order for the computer to use it, it is entirely possible that the programmer may be called upon in difficult cases to enrich the executive's basis for decision making. In this way, the programmer may become privy to very private information about specific individuals. There may then arise a demand for programmers with ethical standards which now are not considered prerequisites to their trade. Inevitably, of course, there will be corruptibles among this group who will leak private information." 221/

219/ Commission to Study the Organization of Peace, The United Nations and Human Rights, Eighteenth Report (New York, 1967), pp. 41-43.

220/ Lord Ritchie-Calder, "Technology and Human Rights", a paper prepared for the Assembly for Human Rights, Montreal, 22-27 March 1968.

221/ Michael, loc. cit., p. 270.

286. The enormous and increasing capacities of the computer heighten the importance of the problem of controlling access to centralized information on individuals, as a protection against threats to privacy. Professor Westin has written:

> "Used to thinking about the problems of storing and using written information, the citizen imagines future data centers as giant installations in huge rooms, with tens of thousands of reels of tape being lifted on and off machines by clerks, and time-consuming human operations required for any significant comparisons to be made of information about a given person scattered through the data bank. In this portrait, time, cost, efficiency, and the requirement of cooperation by considerable numbers of data-bank employees are assumed to provide real limitations on data surveillance. Nothing could be more mistaken...". 222/

287. On the basis of calculations made in several studies by the Rand Corporation in the United States, Westin then shows the rapid growth in computer capacities:

> "Between 1955 and 1965, the size of the central processing unit of the computer decreased by a factor of 10, from 1,000 cubic feet to 100 cubic feet. By 1975, fully integrated circuits will reduce this by a factor of 1,000, to one tenth of a cubic foot.
>
> "Between 1955 and 1965, the internal speed of computers increased by a factor of 200, from 25,000 additions per second to 5 million per second. By 1975, this will be increased another 200 times, making possible operations at the rate of a billion per second.
>
> "In terms of operational costs, the price of doing a million additions declined between 1955 and 1965 from $10 to about 3.5 cents. By 1975, this cost will be reduced by another factor of 300, to one two-hundredth of a cent." 223/

288. The capacities of the computer are likely to grow even more as the result of new developments in data processing. In particular, the development of scanning devices for computerized information will greatly enhance capacities for selectivity in information retrieval, thereby reducing such protection as may be afforded by the volume of information which may otherwise be too unwieldy to handle. For example, the following forecast has been made:

222/ Westin, Privacy and Freedom, p. 166.

223/ Ibid., p. 166.

> "On the horizon in technology is a laser scanning process that would enable a twenty-page dossier to be compiled on each of the 200 million citizens of the United States. Such information could be stored on a single plastic tape reel. Under such conditions, it might be cheaper to retain data than to discard it." 224/

289. It has been further estimated that "specific information from a person's twenty-page dossier could be retrieved in a maximum search time of four minutes, and that the entire dossier could be printed out for dispatch to an inquiring source in a matter of a few more minutes... without platoons of clerks or shifting of storage reels from place to place to signal the operation". 225/

290. Mechanical or technical means of controlling access to data-bank information have been developed and used primarily in connexion with time-sharing systems, i.e., the fast-growing system of renting time for the use of a single large computer to several independent users. As recently as 1966, however, methods of enhancing the privacy of data in a time-sharing system were considered to be "a very poorly studied problem.... There is practically nothing to be found in the computer literature on the subject". 226/ While awareness of the problem has grown since then, only recently has a working system with more than password protection been developed. "In nearly all systems to date, a user's password will get him into his file directory and into any file referenced in that directory." 227/ In such systems information is safe only to the extent that knowledge of the password is limited; this is not a very reliable safeguard in the light of sophisticated eavesdropping and other surveillance techniques. Furthermore, a password system provides only a single barrier at the entrance to the entire filing system, the contents of which may be very broad in scope. For instance, there is no provision for discriminating between "sensitive" information about an individual, which should be protected against access by certain users, and other information.

224/ R.C. Brictson, "Computers and Privacy - Implications of a Management Tool" (Santa Monica, Cal., System Development Corp., 1968), doc. SP-2953/001/00, cited in Lance J. Hoffman, "Computers and Privacy: a Survey", Computing Surveys, vol. 1, No. 2 (June 1969), p. 87.

225/ Westin, Privacy and Freedom, p. 167.

226/ Hoffman, loc. cit., p. 89.

227/ Ibid.

291. It might be supposed that threats to privacy could be reduced by recording information in computers, as far as possible, without reference to an individual's identity. In this way a census agency has access through a statistical data-bank system only to information organized on a category basis. However, it has been maintained by some writers that it is unrealistic and impractical to depend, for much of the statistical storage and calculation desired by governmental agencies and private organizations, on computers having only a limited capacity to identify the individual. Two basic reasons have been given for this. First, many of the advantages, such as economy and availability, accruing from a centralized computer data-bank system are said to be based on the desirability of the integration of information from diverse sources into individually identifiable records in order to correlate even purely statistical information to the fullest advantage. According to Sawyer and Schechter:

> "Even though no scientific interest exists in examining the response of a single individual, it is necessary, in order to compute the over-all relation between, for example, income and education, to match an individual's income with his years of education.
>
> "The requirement for matching means that each individual record in the data centre must be identified, as by a social security number or, better (for guarding privacy), a special code number. Thus is it always theoretically possible to extract from a data centre information referring to a particular individual. This is true whether the centre is characterized as a 'statistical data centre' or as an 'intelligence or dossier file'." 228/

Secondly, the need to keep up to date the information even in a statistical data-bank requires the use of individually identifiable records. Westin writes:

> "The data bank is essentially a pool of information stored in a computer. It may be a static pool, that is, the result of a one-time collection of information, such as the census or a voter survey or the records of a particular social science experiment. This is not the central type of data bank with which we are concerned. Rather we are concerned with what has been called the dynamic data bank, a body of data which is constantly being updated and added to by further collections of data. ...
>
> "Typically, the output of a statistical data bank is data which does not contain identifying characteristics about any individual. However ... the need to keep such statistical data banks updated requires that

228/ Sawyer and Schechter, loc. cit.

identifying characteristics of the individual be retained in the system, so that new and additional data can be added to his file." 229/

292. It should be added that the rapid growth of the capacity of computer systems to digest, store and reproduce information remedies many defects of current filing procedures 230/ and so replaces certain uneconomic and inefficient procedures which have in the past formed natural barriers to the invasion of privacy. Professor Michael has drawn attention to:

"(1) The ability of the privacy invader to bring together data which has been available, but which has been uncollected and uncollated

(2) The ability of the privacy invader to record new data with the precision and variety required to gain new or deeper insight into the private person;

(3) The ability of the invader to keep track of a particular person in a large and highly mobile population;

(4) The ability of the invader to get access to already filed data about the private person; and

(5) The ability of the invader to detect and interpret potentially self-revealing private information within the data to which he has access."

293. Professor Michael continues:

"What is the interplay of these factors and what is their significance for privacy in the light of the computer's capabilities? Much of one's privacy remains undisturbed because no one has had the ability to pull together available information - or because no one has been sufficiently interested to go to the trouble of doing so. To understand the private implications in available data might first require both locating and integrating much widely dispersed information.

"The meaning of the information may be unclear, and therefore, still private. More information may be needed, and the quality of it may depend on updated surveillance of the person involved. Considering the size and mobility of our society, these problems have made privacy invasion very difficult, but ... the computer makes it much more feasible." 231/

229/ Westin, "Discussion Memorandum", pp. 3-4.

230/ Some of these defects are described in detail in E.S. Dunn, "The Idea of a National Data Center and Issue of Personal Privacy", American Statistician, vol. 21 (February 1967), pp. 21-27.

231/ Michael, loc. cit., p. 4.

B. Electronic automation

294. Automation is not necessarily based on electronics, but it has received an enormous impetus from the invention and development of the electronic computer. The problems discussed in this section have been caused mainly by the promotion of automation by the advent of electronic devices, though some may have originated in the earlier days of automation. In general, the intended purpose of electronic automation techniques is the achievement of a socially useful goal such as greater economy or efficiency. Some human rights problems may nevertheless arise.

295. Concern has been expressed with respect to protecting the dignity of human labour in the light of electronic automation. It was maintained in the Third Committee of the General Assembly at its twenty-third session that it was impossible to speak of the dignity of human labour when developments in electronics made it feasible for industries and organizations to be administered by advanced cybernetics.[232/] At the International Conference on Human Rights, Teheran, April-May, 1968, the view was expressed that within the next few decades one of the greatest preoccupations of man would be to protect his physical integrity and moral dignity against the effects of automation.[233/]

296. Computer-spurred automation has had an impact on employment levels and work patterns.[234/]

297. Donald F. Hornig, Director of the United States Office of Science and Technology, described the effect on labour of the rapidly increasing reliance upon computers:

> "In the process, many people are either going to have to learn to do new jobs, or we'll have severe social problems. As the computer makes it possible to automate industries and to do tasks, it's going to provide new jobs, but they're going to require a higher level of skill and education from our people if they're going to be in command of the computers instead of the computers in command of them.....
>
> "These problems are all soluble ones. But if they aren't met, then we're then we're going to have disaffected people who have been displaced from their jobs, socialoorganizations which have been disturbed." [235/]

232/ Official Records of the General Assembly, Twenty-third Session, Third Committee, 1642nd meeting, p. 3.

233/ A/CONF.32/C.2/SR.9, p. 104.

234/ A tendency referred to by Westin in Privacy and Freedom, p. 298.

235/ Radio script entitled "The Circumstance of Science", broadcast in September 1968 by Michigan State University Radio, Michigan, United States of America.

298. The Assembly for Human Rights which met in Montreal, 22-27 March 1968, drew attention to the "danger of the 'human cassette', the computer training of workers for specific, short-term functions and their discarding when they have fulfilled their limited usefulness".236/

299. Professor Sohn, of Harvard University, has stated the following in relation to the social implications of computer-based technological developments:

> "When the right to work is cut down conspicuously by machines, and when those who operate the machines need more and more sophisticated training, the right to a new type of education becomes crucial. Anybody who cannot receive the new training or is intellectually unqualified for it, becomes an outcast in the community, whose survival is imperiled unless he is continuously subsidized in doing nothing or in performing unnecessary tasks. A community of drones cannot survive long without a rebellion against the social order which has deprived them of a meaningful existence. The right to leisure, attractive in small doses, becomes a bore quite quickly. Our society has already encountered a great difficulty in dealing with the growing number of retired people. What is going to happen in a world where most people work only part-time or retire early, after only a few years of work? The whole structure of the society will have to be revised in this new era when not only all unpleasant work is performed by machines but in which even most of the intellectually stimulating work can be performed better by mechanical devices." 237/

C. Other uses of computers

300. To an increasing extent business and governmental leaders are using computers to "decide" questions that call for value judgements rather than fact or trend analysis.238/ The possible impact on democratic institutions of the growing use of computers for decision-making have been described as follows:

> "What is going to happen to human rights in a world which is becoming so complicated that more and more important decisions have to depend on computers and other machines? There is a grave danger that actual decision-making will be no longer in the hands of duly elected representatives of the people but instead in the hands of those who feed the data to the computers on which decisions are based and who are the interpreters and implementors of the answers given by the computers. New arrangements will have to be devised

---

236/ Montreal Statement of the Assembly for Human Rights (Montreal, 1968), sect. IX.

237/ Louis B. Sohn, in a paper delivered before the Center for International Studies, New York University.

238/ A tendency referred to in Westin, Privacy and Freedom, p. 298.

> to control the precious few who know how to run the machines, and on whose wisdom and impartiality the fate of mankind may depend. Many military decisions already depend on answers given by computers, and many experts are working hard on programming computers for work in many crucial areas where decisions might directly impinge on the well-being of vast groups of individuals. Before they go too far, new safeguards need to be developed to protect the rights of individuals and of their elected representatives." 239/

301. Reference may be made at this point to the increasing use of the computer by social scientists. It has been said that the computer

> "provides /the social scientist/ with the means for combining in complex models as many variables as he needs in order to simulate the behaviour of men and institutions. Previously the behavioural scientist simply could not deal with as many important variables as are needed to understand and predict human behaviour. From now on he will increasingly be able to do so." 240/

For instance, the development of scientific urban planning has been promoted by the use of the computer.241/ As regards the impact of the computer in the area "social engineering" and the questions it raises, Professor Michael has written:

> "the computer has a unique capacity for collecting and processing enormous amounts of data about the state of individuals and of society today - not that of ten years ago. Thus, the behavioural scientist not only can know the state of society now as represented by these data, but he can use them to test and refine his theoretical models. The convergence of government programs and the computer is of critical importance; it will result in an efflorescence of longitudinal studies of individual and institutional change

---

239/ Commission to Study the Organization of Peace, op. cit., p. 41.

240/ Donald N. Michael, "Social Engineering and the Future Environment", American Psychologist, vol. 22, No. 11 (November 1967), p. 889. See also, for example, Davis B. Bobrow and Judah L. Schwartz, Computers and the Policy-making Community: Applications to International Relations (Englewood Cliffs, New Jersey, Prentice-Hall, 1968).

241/ See, for example, Jay W. Forrester, Urban Dynamics (Cambridge, Massachusetts, Massachusetts Institute of Technology Press, 1969); New York Times (31 October 1969), p. 47; Sergei N. Grimm, "The Scientific Urban Planning System"; Law and Computer Technology, The World Peace Through Law Center, Geneva, vol. 2, No. 1 (January 1969), p. 19.

as functions of the changes in the social and physical environment. Such knowledge, now essentially non-existent, will inevitably increase our ability to effect social change. And given the convergence of the powerful technologies and our already enormously complex and huge society, it would seem that social manipulation will be necessary if we are to introduce appropriate changes in society at the appropriate times. The problem, of course, is: Who is to decide who is to be manipulated and for what ends?" 242/

302. Concern has been expressed with respect to the undue influence of technological considerations in decision-making processes traditionally dominated by other factors. For example, M. Guy Braibant, Maître des requêtes au Conseil d'Etat and Secrétaire général de l'Institut français des Sciences administratives has made the following observation on the use of the carte d'identité in France:

"The other aspect, of which we have a recent example, is the case where political decisions are taken for technological reasons. The reader may have seen in the newspapers in early January 1969 an announcement by the Ministry of Finance, to the effect that any person wishing to secure foreign currency must have an exchange passbook and that to obtain such a passbook he must produce a national carte d'identité. The official reason given was that the computers used for exchange control could identify and process only carte d'identité numbers. This is an indirect way of enforcing something which is merely optional. The carte d'identité problem is essentially a political and legal one; thus it happens that, by a kind of circuitous route, a situation occurs in which a technical service has imposed a political decision for purely technical reasons." 243/

303. The tendency of the use of computers to promote depersonalization prompted Lord Ritchie-Calder, in his paper prepared for the Assembly for Human Rights, to observe: "We are ceasing to be people and are becoming statistics. To the authorities we have no names, no faces and no personality. We are becoming code numbers in the computer."

242/ Donald N. Michael, "Some Speculations on the Social Impact of Technology", p. 10, reprinted chapter from Technological Innovation and Society, Dean Morse and Aaron Warnet, eds. (New York, Columbia University Press, 1966).

243/ Guy Braiband, "L'informatique dans l'administration", Institut International des sciences administratives, Table Ronde de Barcelone (June 1969), p. 5, communicated by the Institute to the Secretary-General.

D. Electronic communications media

304. The rapid development of the media of mass communications has increased concern over the misuse of the media for propaganda, advertising and similar purposes to the benefit of the small number of persons in control of those media. A recollection of the effective political use of the radio by the nazi régime will indicate that this is not a new problem. What gives it special importance today is the greatly increased influence of the mass media, particularly television. The International Catholic Child Bureau, in its contribution to the present study dated 12 May 1969, provided an example of the concern which is felt regarding this issue:

> "It is important that those who have at their disposal the technological means of influencing education and private and public opinion are made aware of their responsibilities. The intellectual, spiritual, cultural and moral progress of humanity must be fostered by scientific and technical advancement, but it is important that future developments be properly administered since there is a danger that pressures could be created by such advances which could diminish human capacities and the freedom of the individual."

305. A more particular problem, applicable to television and to radio (and to films), is that of the subliminal message which, as was observed in the Third Committee of the General Assembly at its twenty-third session, could be incorporated in cinema or television film and so penetrate the subconscious.[244/]

306. On the recommendation of its Legal Committee, the Consultative Assembly of the Council of Europe at its nineteenth ordinary session adopted, on 31 January 1968, recommendation 509 (1968),[245/] on human rights and modern scientific and technological developments. In the third preambular paragraph to this resolution, the Consultative Assembly expressed its belief "that newly developed techniques such as... subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by article 8 of the European Convention on Human Rights". In the relevant report of the Legal Committee to the Consultative

---

244/ Official Records of the General Assembly, Twenty-third Session, Third Committee, 1642nd meeting, p. 4.

245/ On this recommendation, see also para. 61.

Assembly (document 2326 of 22 January 1968), reference was made to "the new technique which projects photos many times on a screen for less then 1/16 second during the performance of a moving picture. Due to the shortness of time, the contents of such photos are not taken notice of consciously; yet they exert a decisive influence on people as has been proved by experiments. This constitutes an immense danger in political and other respects".

307. Subliminal messages "the projection of messages by light or sound so quickly and faintly that they are received below the level of consciousness", 246/ have been proved very effective on an experimental basis in commercial advertising. Lord Ritchie-Calder has stated:

> "There are subliminal and brain-washing techniques by which the subconscious of the individual is invaded and his thoughts or personality influenced without his consent. These influences can be smuggled in past the customs of the senses. Methods of which I am aware include ultrasonic waves. These are inaudible to the conscious senses, like the 'silent' dog-whistle inaudible to man. At sonic frequencies just beyond the threshold of normal hearing an insidious and persistent silent message can, at unsuspecting moments, get through to the subconscious - like the signal of an unfamiliar radio-station impinging on a neighbouring wave-band. Similarly subliminal messages can be concealed in films or television programmes. Of course, such means are banned but anyone sufficiently ingenious, or some central authority seeking to indoctrinate, could succeed.... I have seen television commercials which I strongly suspected of employing subliminal. Unless one could investigate at the point of preparation, it would be difficult to establish this intrusion because by very definition the conscious senses would not recognize it; it would be subliminal at the receiving end, and therefore undetectable." 247/

308. There are many future possibilities for the abuse of the communications media, for example, the possibility of hypnotizing persons watching television, as has been demonstrated in experiments. 248/

246/ Westin, Privacy and Freedom, p. 279; evidence of their use appears on pp. 279-297 of the same work.

247/ Ritchie-Calder, "Technology and Human Rights", a paper prepared for the Assembly for Human Rights, Montreal, 22-27 March 1968.

248/ Westin, Privacy and Freedom, p. 297, states that Dr. Herbert Spiegel and Dr. James H. Ryan of the College of Physicians and Surgeons of Columbia University, New York, demonstrated such experiments at the American Medical Association Convention in 1965.

2. Studies made or in progress

309. On 29 October 1969, the Government of Canada stated that it was co-operating in the sponsorship of a seminar on computers and personal privacy to take place in the spring of 1970. The Government added:

> "The Department of Industry, Trade and Commerce is also co-operating in a study being undertaken in the OECD Committee for Science Policy on Computer Utilization in member countries. This study covers the following topics: (a) the value of existing computer surveys; (b) the establishment of commonly agreed standards for the collection of statistical data on computer utilization; (c) the compilation of a directory of points of contact in member countries for detailed information about computer usage in specific areas; and (d) the qualitative aspects of computer utilization in management information systems, computer-based data banks in the public sector, and the problems of the misuse of stored individualized data, that is, the protection of privacy."

310. The Government of Canada also forwarded the following information on a private study which is under way:

> "Privacy and the computer: Director of research, Professor J.M. Carroll, Associate Professor, Department of Computer Science, University of Western Ontario, assisted by Professor J.I. Williams, Department of Sociology, and Professor E.F. Ryan, Faculty of Law of the University of Western Ontario. The project is intended as an investigation of the potential of large computer-based data banks for invading individual privacy and the means which are available to reduce the likelihood of this invasion. The first objective is to study files of student records maintained by universities. The investigation will be expanded in steps to include files of records relating to medicine and psychiatry, secondary education, criminal justice, welfare, land use, retail credit and insurance. The investigators intend to determine the norms of current practice with regard to data elements stored and the administrative and technical procedures for updating, releasing, validating and purging data. They will also determine the degree to which interchange of information takes place between data centres and investigate the protection of data communications channels from unauthorized interception. They plan to propose safeguards of individual privacy in such areas as federal and provincial law, file organization and management, computer operating systems and procedures, cryptographic systems and special data communications equipment."

311. On 15 September 1969, the Government of Denmark, in addition to referring to a general study in progress relating to the protection of privacy of individuals in the light of technological advances,[249] wrote:

249/ See para. 38.

"The National Health Service has set up a working group dealing with electronic data processing of patient and treatment statistics in connexion with the further development of individual patient statistics. The study group has considered the question of protecting the individual against abuse, for instance by the police and the Press, of such registered data."

312. On 6 November 1969, The Government of Sweden forwarded to the Secretary-General information on a Royal Commission appointed in 1966 to elaborate legislative proposals concerning the protection of privacy in general against invasion by modern scientific and technical devices.[250] The Government added:

"in 1969, two Royal Commissions have been set up to inquire into, i.a., the need for special safeguards to ensure that EDP /electronic data processing/ -techniques are not used in ways that would be detrimental to personal integrity. One of the Commissions shall make a study of publicity and secrecy. According to its terms of reference it shall also examine the need for new secrecy-rules in respect of the application of EDP-techniques in public administration. The other Commission has been instructed to study the future organization of the credit information activity. The Commission should make recommendations for regulating this activity in such a way as to protect the integrity of individual citizens and to improve the structure of this branch. It has been stressed that the development in recent years in the field of EDP has had a considerable impact on this branch due to increasing possibilities of collecting and systematizing information of different kinds."

313. In its contribution to the present study dated 17 December 1969, the Government of the United Kingdom stated:

"On the question of the use of competers and human rights, with particular reference to the storage of medical data by computer, certain rules have been laid down by the National Data Processing Service (NDPS) in the United Kingdom. The NDPS is concerned with the use of computers and the need to protect its customers from unauthorized disclosure of information concerning their affairs. To this end provision has been made in the Post Office Act, which was enacted earlier this year, for NDPS staff, together with the staff of the other Post Office businesses, to be subject to legal penalties if customers' information is wrongly disclosed. Other bodies in the United Kingdom have been considering the problems of confidentiality posed by the rapid development of computer systems. In particular, the British Computers Society has recently set up a Computer Privacy Group, in which the NDPS is represented, to review and make recommendations on the maintenance of privacy and confidentiality in relation to data records and the security requirements of personal and

---

250/ See para. 42.

organizational records where such records are in the custody of electronic data-processing facilities, or are in transmission between a remote point and such facilities. The Computer Privacy Group will also make recommendations on the management of confidential information in electronic data-processing facilities through the use of administrative techniques, legal sanctions, technical methods and the development of ethical standards."

314. On 1 December 1969 the Government of the United States of America drew attention to the following two reports on relevant inquiries by the United States Congress:

"U.S. Congress. House. Committee on Government Operations.

Special Subcommittee on Invasion of Privacy. The computer and invasion of privacy. Hearings before the Special Subcommittee, 89th Congress, 1st Session, July 26-28, 1966. Washington, D.C., U.S. Govt. Print. Off., 1966. 318 p.

"U.S. Congress. Senate. Committee on the Judiciary.

Subcommittee on Administrative Practice and Procedure. Computer privacy. Hearings before the Subcommittee. 90th Congress, 1st Session, March 14-15, 1967. Washington, D.C., U.S. Govt. Print. Off., 1967. 269 p."

315. A meeting of experts scheduled to meet in January 1970 under UNESCO auspices[251/] was to examine, inter alia, the impact on human rights of the use of computers.

316. Within the Council of Europe, the adoption of recommendation 509, on human rights and modern scientific and technological developments, by the Consultative Assembly on 31 January 1968, and the inclusion by the Committee of Ministers in April 1968 of the same subject in the Council's intergovernmental programme of work for 1968/1969, have already been referred to.[252/] With respect to electronic data processing in particular, the Council of Europe forwarded the following information on 9 June 1969:

251/ See para. 56.

252/ See paras. 61-62.

"the Committee on Science and Technology of the Consultative Assembly is examining the subject 'Science, Technology and Human Rights', with particular reference to the problem of data processing and human rights. On 24 April 1969 this Committee held a meeting in Stockholm, at which several Swedish experts and members of the Committee held a first exchange of views on this subject.

"Moreover, in recommendation 557 of 14 May 1969, on the use of computers in local government, the Assembly drew attention to the dangers for the rights and freedoms of the individual resulting from the use of computers and recommended that adequate laws and regulations should be drafted to ensure the necessary protection in this respect."

317. In the United States of America, the issue of privacy in relation to a large centralized data bank centre has been widely discussed as a result of proposals which have been made to establish a national data centre, bringing together in one place, for storage and dissemination, governmental information on individuals at present gathered for a variety of purposes and kept in separate places.[253/] Some study has been accorded to techniques to provide security against misinformation and to restrict access to data banks to authorized users.[254/] There is also available an annotated bibliography on the subject of the protection of privacy in the computer age.[255/] As a part of the Harvard University Program on Technology and Society, a study is in progress by Professor Alan Westin on "information technology and public decision-making".[256/]

253/ This discussion is reviewed in Sawyer and Schechter, "Computers, Privacy and the National Data Center: the Responsibility of Social Scientists", American Psychologist, vol. 23, No. 11 (November 1968), pp. 812 et seq.

254/ See, for example, Paul Baran, "On Distributed Communications: IX. Security, Secrecy, and Tamper-free Consideration", Memorandum RM-3765-PR (August 1964), Rand Corporation, Santa Monica, California.

255/ Annette Harrison, "The Problem of Privacy in the Computer Age: an Annotated Bibliography", Memorandum RM-5495-PR/RC (December 1967), Rand Corporation, Santa Monica, California.

256/ Harvard University Program on Technology and Society, Fourth Annual Report (Cambridge, Massachusetts, 1968), pp. 32-34.

318. In the United Kingdom, also, there has been discussion of the human rights problems arising from the growing use of computers, and some legislative and other proposals have been made for meeting these problems. For example, the National Council for Civil Liberties, which has taken a considerable interest in the matter, published in 1968 a pamphlet by Donald Madgwick, which included a proposal making the consent of the individual concerned a prerequisite for the recording in a computer of information about him.257-258/

319. The effects of automation have been discussed in publications of the International Labour Office, including articles in International Labour Review, among them, H. de Bivort, "Automation - Some Social Aspects", International Labour Review, vol. LXXII, No. 6 (December 1955), p. 467; International Labour Conference, fortieth session, Report of the Director-General, Part I: Automation and Other Technological Developments - Labour and Social Implications (Geneva, 1957); and the Labour and Automation Bulletin Series (published from 1964 onwards). An account of the automation programme of the ILO is included in "Economic rights and opportunities for women - ILO activities related to repercussion of technological change on employment and conditions of women workers: report by the International Labour Office" (E/CN.6/500) of 6 December 1967.

320. Effects of automation upon aspects of employment are discussed by Dr. Avner Hovne in "Some Social Implications of Automation", Impact of Science on Society, vol. XV, No. 1 (1965), pp. 5-25, issued by the United Nations Educational, Scientific and Cultural Organization.

321. As regards subliminal suggestion, the Government of the United Kingdom has stated:

> "On the question of human rights in advertising, the Institute of Practitioners in Advertising (the trade association of advertising agencies in the United Kingdom) has condemned subliminal advertising and the use of hypnosis as advertising techniques. Subliminal advertising is banned from television by Section 3 (III) of the Television Act 1964. Under this Act the Independent Television Authority must satisfy themselves that the programmes broadcast by the authority do not include any technical device which, by using images of very brief duration or by any other means, exploits the possibility of conveying a message to, or otherwise influencing the minds of, members of the audience without their being aware, or fully aware, of

257-258/ Donald Madgwick, Privacy under Attack (London, 1968), especially pp. 32 et seq. and 40.

what has been done. This prohibition of subliminal transmission applies to television broadcasting as a whole and not only to television advertisements. The British Broadcasting Corporation (B.B.C.) is also prohibited from using this type of television broadcast."

3. Proposed further surveys

322. From paragraphs 309-321 above it is clear that attention is being given to human rights problems arising from the increasing use of computers, and especially to the question of privacy. It will be possible for the survey to be made in accordance with General Assembly resolution 2450 (XXIII) to take into account much that has already been written, including a certain number of proposals for the protection of privacy.

323. It is suggested that studies may be needed in relation to:

(i) The possibility of registration and public control of operators of data-bank centres;

(ii) The question of adequate selection and training of computer programmers;

(iii) The question of reducing the possibility of error as a result of malfunctioning by a data-bank system;

(iv) The right of the individual to be informed of what is recorded concerning him and to have inaccurate information removed;

(v) The various ways in which access to a data-bank system may be controlled;

(vi) The effect on the political life of the nation of the concentration in data banks of knowledge concerning individuals;

(vii) The dangers that may arise from subliminal suggestion through electronic communications media and what might be done to counter them.

IV. OTHER PROBLEMS IN CONNEXION WITH HUMAN RIGHTS ARISING FROM DEVELOPMENTS IN SCIENCE AND TECHNOLOGY

1. General remarks

324. Paragraph 1 of General Assembly resolution 2450 (XXIII) requires the problems in connexion with human rights arising from developments in science and technology to be studied, "in particular" from the standpoints reflected in the headings to chapters I, II, III, and V of the present report. In the Third Committee of the General Assembly at its twenty-third session, several representatives stressed that paragraph 1 of resolution 2450 (XXIII) listed only some examples of the problems involved and was not to be considered exhaustive.[259/] The present chapter refers to some topics, other than those dealt with in chapters I-III, which may call for a degree of treatment, in order to permit of implementation of paragraph 1 (d) of the resolution, which invites the Secretary-General to study "the balance which should be established between scientific and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity". A general view of all human rights problems arising out of scientific and technological developments would seem to be necessary also for the drawing up of "appropriate standards to protect human rights and fundamental freedoms", for which the present study may be the basis, according to the third preambular paragraph to General Assembly resolution 2450 (XXIII). The problems referred to in the present chapter have been and are being studied extensively elsewhere; the Secretary-General proposes, not to duplicate any studies already made or in progress but, as far as possible, to refer to such studies.

325. It may be in order to recall at this point that, while the present preliminary report speaks of threats and dangers to human rights arising out of scientific and technological developments, the later study which is called for by paragraph 1 of General Assembly resolution 2450 (XXIII) might take into account also the benefits of such developments, so as to be able to assess their advantages and disadvantages in the light of the intellectual, spiritual, cultural and moral advancement of mankind. This sesms to be an appropriate point at which to recall this fact

---

259/ Official Records of the General Assembly, Twenty-third Session, Annexes, agenda item 62, document A/7433, para. 149.

because of the essential difference between some of the problems dealt with in the present chapter and some of those treated earlier. For instance, the abuses of surveillance devices are deliberate acts, whereas the deterioration of the human environment has been a by-product, until recently generally regarded as inevitable, of the interference with the environment which was necessary for the realization of the right of everyone to "a standard of living adequate for the health and well-being of himself and his family", laid down in article 25 (1) of the Universal Declaration of Human Rights. Similarly, the problems created by the population explosion are a by-product of the wider enjoyment of health, including the declining death rate of people before reaching the age of procreation.

2. Deterioration of the human environment

326. In its contribution to the present study, the Government of the Federal Republic of Germany has stated:

> "Technological development... constitutes a threat to a man's immediate environment. The problems involved are similar in all countries that have achieved a comparable level of economic, technological and scientific development. They include air and water pollution, noise, traffic congestion, the biological effects of chemical products, the settlement of open areas...".

327. The following are among the responses received by the Secretary-General to his invitation extended to various bodies, to contribute to the present study:

(i) On 6 June 1969, UNESCO sent the conclusions of a symposium on science policy and biochemical research, organized by the Council for International Organizations of Medical Sciences, under the sponsorship of UNESCO and WHO, and held 22-29 February 1968. This includes a section entitled "Man's environment";

(ii) On 3 July 1969, WHO sent a provisional memorandum, which, inter alia, referred to "some of the relevant research projects in the period 1964-1968, identified within broad areas of the Organization's activities", including:

"Environmental Pollution - studies of water, air, soil and radioactive pollution in an effort to prevent pollution from reaching levels which interfere with the health and well-being of individuals.

"Wastes Disposal - research and establishment of scientific and technical information on wastes management and control.

"Vector Biology and Control - assessment of the safety of pesticides and of methods of aircraft disinsection."

(iii) On 5 May 1969, the International Association of Democratic Lawyers sent the agenda of the Congress of the Association to be held in the spring on 1970, which includes the following item:

"IV (d) Legal protection against the pollution and deterioration of the human environment".

328. These replies have recognized the importance from the point of view of human rights of a problem which is causing increasing concern in many sectors of society, especially in some of the more populous countries: the deterioration of the human environment due to scientific and technological developments. This problem is the more serious because the harmful environmental by-products of these developments are often unpredictable and because the developments have been so rapid. It is relevant to the present study because the deterioration in the environment (i) is a threat to the right to life, which is proclaimed in article 3 of the Universal Declaration of Human Rights, (ii) infringes article 25 (1) of the same Declaration, according to which, "Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food" and (iii) reduces the enjoyment of living of millions, the right to which is implied in the reference to an adequate standard of living which appears in article 25 (1) of the Declaration and in the mention of the dignity and worth of the human person which appears in the preamble to that instrument.

329. The General Assembly, in paragraph 1 of its resolution 2398 (XXIII) of 3 December 1968 on the problems of human environment, decided to convene a United Nations Conference on Human Environment in 1972. In the first four preambular paragraphs of that resolution, the General Assembly recognized the link between human rights and the impairment of the human environment:

"The General Assembly,

"Noting that the relationship between man and his environment is undergoing profound changes in the wake of modern scientific and technological developments,

"Aware that these developments, while offering unprecedented opportunities to change and shape the environment of man to meet his needs and aspirations, also involve grave dangers if not properly controlled,

"Noting, in particular, the continuing and accelerating impairment of the quality of the human environment caused by such factors as air and water pollution, erosion and other forms of soil deterioration, waste, noise and the secondary effects of biocides, which are accentuated by rapidly increasing population and accelerating urbanization,

"Concerned about the consequent effects on the condition of man, his physical, mental and social well-being, his dignity and his enjoyment of basic human rights, in developing as well as developed countries".

330. The following summary of relevant aspects of the deterioration of the human environment is based principally upon an examination of the debate in the General Assembly at its twenty-third session which led to the adoption of the above-mentioned resolution (A/PV.1732-1733):

(i) A threat to health and even life is posed by the pollution of the air due to industrial activity, traffic, domestic heating and other factors. Nuclear blasts, for whatever purposes, peaceful or otherwise, and experiments with biological and chemical methods of warfare also create hazards to health and life;

(ii) Psychological and physical damage and a general deterioration in living comfort are caused by the increase of noise in the urban environment; causes of this include increased air traffic, supersonic travel with the accompanying supersonic boom, increased street traffic and demolition and construction activities;

(iii) A threat to health, to the enjoyment of the amenities of life and to the continued supply of essential raw materials is posed by excessive waste creation and inefficient waste disposal, including the dangers arising in connexion with the disposal of the wastes of nuclear power sources.

(iv) There are various threats to the world food supply which also entail in some measure an impairment of mankind's more general enjoyment of.

the amenities of life, including the visual beauty of the landscape. These include erosion and other forms of soil deterioration; water pollution by domestic sewage, industrial wastes, drained-off chemical fertilizers and pesticides and thermal pollution; other harmful secondary effects of pesticides, other biocides, chemical fertilizers and synthetic detergents; and the increased danger of oil pollution of shores due to off-shore oil drilling and the use of larger oil tankers, which do great damage in case of wreck.

331. Some of these hazards affect in some measure the whole of humanity. Others are essentially problems of urban living. Increasing population and accelerating urbanization exacerbate many of the dangers referred to. In addition, attention has been drawn to the individual's possible loss of identity in huge cities and conurbations and to the threats to his psychological stability due to overcrowding there.

332. These problems concerning the human environment, and possibly others of concern to human rights, may be discussed at the conference to be held in 1972 under General Assembly resolution 2398 (XXIII). The report of the Secretary-General on problems of the human environment (E/4667, paras. 1-50), of 26 May 1969 provides an indication of topics likely to be discussed at that conference; it also includes references to studies already made or in progress which are relevant to the subject-matter of that conference, and it contains proposals for the preparation of documentation for the conference. To the extent that the preparatory work for and the discussions at the 1972 conference which deal with problems affecting human rights may be advanced before the study requested under paragraph 1 of resolution 2450 (XXIII) is completed, it will be unnecessary for that study to do more than refer to them.

3. The population explosion

333. The world is witnessing an explosive increase in population that is due partly to advances in medicine and is giving rise to increasing problems in relation to adequacy of food supplies, living space and economic resources in general. This has been one of the concerns of the United Nations Population Commission and the Economic and Social Council. Mr. Gordon Taylor has observed

that it is impossible to expand agriculture fast enough to meet the current population expansion, "for population grows geometrically, whereas agriculture can only be increased arithmetically".260/ At the discussion on surgical ethics, with special reference to the problems arising from transplantation, organized by the International Federation of Surgical Colleges and held on 28 September 1966 in the Polish Academy of Science, Warsaw, Sir John Bruce, Regius Professor of Surgery at the University of Edinburgh, mentioned some causes and results of the population explosion in connexion with organ transplants:

> "We are faced in the world of today with an enormous population explosion. By the end of this century, the inhabitants of the earth will have doubled, and already more than half of the present population are living below the 'bread line'. Some part of this difficulty has been created by medical and paramedical advances - for example, the control of malaria, and other epidemic diseases in various parts of the world. Is it justifiable to keep on trying to salvage, at great cost, more and more victims of chronic and irremediable diseases? Perhaps the doctor standing in a personal and emotional relationship to individual patients is not the right person to supply the answer." 261/

4. Increasing destructive power of modern weapons

334. Modern science and technology is recognized as having rendered possible vast suffering and perhaps even the annihilation of the human race through the destructive power of modern weapons. This poses a threat to all human rights. The contribution of the International Commission of Jurists to the present study includes the following:

> "Lastly, there can be no doubt that one of the 'scientific advances' physically most harmful to the human person is the prodigious development of armaments, the immediate or insidious effects of which may cause the death of non-combattants and suffering which may last many years, and may even cause physical harm to unborn children by contaminating their future parents."

260/ Gordon Rattray Taylor, The Biological Time Bomb (New York, 1968), p. 56.

261/ International Federation of Surgical Colleges, News Bulletin, No. 7 (May 1966), p. 18, furnished by the Federation.

335. The wording of that passage shows that the Commission had atomic weapons in particular in mind. Apart from the possible use of such weapons in warfare, atomic radiation poses hazards to mankind, as is mentioned in paragraphs 337-338.

336. A particular reference should also be made to the report of the Secretary-General, Chemical and bacteriological (biological) weapons and the effects of their possible use (United Nations publication, Sales No.: E.69.I.24), which describes, inter alia, the short-term and long-term effects upon man of the use of such weapons. The dangers of such weapons are receiving widespread discussion. It is sometimes claimed that the mere manufacture, storage and transport of such weapons are a threat to health and life, in view of their highly toxic effects in the event of accident.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

COMMUNICATION

PANEL 4

Réglementation des systèmes d'information: objectifs, moyens et coûts

par

Calvin C. Gotlieb

Université de Toronto

CONFERENCE

SUR

L'ORDINATEUR, LA VIE PRIVEE ET LA LIBERTE D'INFORMATION

UNIVERSITE QUEEN'S

21-24 MAI

1970

Réglementation des systèmes d'information: objectifs, moyens, et coûts

par

Calvin C. Gotlieb
Université de Toronto

Résumé

L'auteur propose une classification des sytèmes d'information qui permettrait l'identification des sytèmes qui peuvent poser des problèmes de sécurité ou menacer le caractère confidentiel des données. Il examine les coûts que suscite une réglementation, coûts directs quand il s'agit du hardware, coûts indirects en ce qui concerne l'élément plus complexe que devient le software et coûts prohibitifs attribuables aux restrictions qui empêchent l'exercice de certaines activités. L'auteur conclut qu'en dépit des problèmes et des coûts connexes à une réglementation, la loi canadienne devait reconnaître explicitement la notion de droit à la vie privée. Il recommande que des licences soient délivrées pour l'exploitation de certains systèmes d'information. Il suggère que soient encouragées les innovations techniques qui permettraient une sécurité et un contrôle plus grands dans le transfert des informations.

Réglementation des systèmes d'information: objectifs, moyens et coûts

par

Calvin C. Gotlieb
Université de Toronto

1. Position de la question

Les documents de fond distribués aux participants placent dans sa propre perspective le dilemme qui se pose dans le titre de cette conférence. En voici les éléments principaux:

(i) Les systèmes d'information sont de plus en plus nécessaires

Les systèmes d'information concernant l'individu sont de plus en plus nécessaires dans le secteur public (recensement, rapports d'impôt, statistiques médicales, enquêtes de police, etc.) et dans le secteur privé (filières de banque, de crédit, d'assurance, etc.). Les gouvernements ont besoin de cette documentation pour se décharger de leurs obligations; les planificateurs et les sociologues en ont besoin pour comprendre notre société et proposer les mesures appropriées à sa bonne orientation; enfin, nos hommes d'affaires en ont besoin pour bien administrer leurs exploitations et leurs services.

(ii) Nous évoluons vers les systèmes intégrés

Nous nous acheminons vers l'emploi des sytèmes intégrés, c'est-à-dire les systèmes contenant des renseignements hétérogènes sur plusieurs personnes et dont les données sont accessibles à différentes autorités à des fins différentes. De tels systèmes sont fortement prisés parce qu'ils permettent

de rassembler des données plus précises et plus constantes, en plus d'être moins coûteux et d'offrir une gamme plus complète de données.

(iii) La loi protège peu contre les abus dans l'usage de l'information

Le concept du droit à la vie privée est très mal défini dans la loi canadienne. L'on ne trouve que dans quelques circonstances, seulement, des règlements stipulant le genre d'agence qui a le droit de recueillir tel genre d'informations, la façon dont les renseignements doivent être vérifiés et à qui il est permis de les transmettre. L'individu ne bénéficie donc d'à peu près aucune protection contre les abus d'information dont il peut être la victime.

(iv) L'avènement de l'informatique accroît le danger du manque de protection juridique

Les progrès de la technologie dans les méthodes de stockage et les appareils de communications permettent de mettre au point des systèmes d'information intégrés basés sur des banques de données établies par ordinateurs. L'accessibilité des terminaux et la facilité de communication accroissent le danger que des renseignements concernant un individu soient divulgués à tout hasard et sans égard pour ses intérêts légitimes. D'autant plus que ce danger est souvent aggravé par une confiance injustifiées portée aux données informatiques.

(v) Les mesures pour régir des banques de données sont parfois controverse

Ces observations aboutissent logiquement à la mise au point de mesures de réglementation des banques de données, comme par exemple l'obtention d'une licence; de telles propositions sont énoncées dans les travaux qui serong présentés à cette conférence. Les adversaires de la réglementation soutiennent qu'en général, ces mesures ne produisent pas les résultats escomptés et sont, de toute façon, impossibles à faire respecter. Par contre, les protagonistes de telles mesures affirment que ces dernières sont essentielles à la sauvegarde des droits humains et qu'elles doivent être adoptées avant qu'il ne soit trop tard.

Quant au présent travail, il accepte le principe d'une certaine forme de réglementation. La plupart de ceux qui assitent à cette conférence ont sans doute des opinions bien formées à ce sujet et ne changeront probablement pas d'idée par suite de nos délibération. À mon avis, le coeur de la question est le suivant: est-il possible de formuler et de mettre en vigueur des règlements efficaces? Plusieurs adversaires de la réglementation affirment que l'informatique fait partie si intégrante de notre technologie qu'il est impossible de la restreindre, que toute réglementation susceptible d'assurer le droit à la vie privée occasionne une perte inacceptable d'efficacité et de rendement, et

qu'une certaine atteinte au caractère privé de la vie individuelle est inévitable. Nous ne partageons pas ce point de vue. Notre propos est plutôt d'examiner nos objectifs et de montrer que l'adoption de mesures propres à les atteindre n'est pas quasi impossible.

2. Objectifs

Il n'est pas malaisé d'énumérer des objectifs qui sont, en soi, des évidences, comme, par exemple:

- Le droit à la vie privée doit être respecté le plus possible, tout en tenant compte des besoins légitimes de la société.
- Les informations concernant l'individu doivent être aussi exactes que possible.

Là où se pose la difficulté, c'est dans l'interprétation d'expression particulières comme "droits individuels" et "besoins légitimes de la société", employées dans le contexte des projets de réglementation proposés.

Le premier objectif mentionné laisse entrevoir les deux concepts en jeu: droit à la vie privée, d'une part, et liberté d'information, de l'autre. Il présuppose qu'un individu ne peut refuser à la société le pouvoir de compiler certains informations à son sujet, comme, par exemple, son certificat de naissance et sa fiche de sécurité sociale.

Mais il présuppose aussi qu'il existe des droits au caractère privé de la vie individuelle. Puisqu'il est généralement reconnu* que la loi est très vague à ce sujet, il s'ensuit qu'il importe de formuler une législation définissant le droit à la vie privée. C'est là un point essentiel. Si je ne m'y attarde pas, c'est que je ne me considère pas suffisamment expert pour discuter de la place que doit occuper une telle législation dans notre code; doit-elle, par exemple, comme le propose Ryan, faire partie de la loi provinciale ou fédérale, ou des deux, ou encore dans quelles parties du code vaut-il mieux l'intégrer? J'espère que des projets de loi spécifique seront avancées au cours de cette conférence.

Bien que nécessaire, le concept juridique du droit à la vie privée ne suffit pas. Il faut aussi considérer l'interprétation de ce concept dans l'application des systèmes d'information. Il importe, en particulier, de relier ce concept aux règlements auxquels devront se conformer, dans l'emploi de données, ceux qui sont chargés de mettre sur pied, de rassembler et de faire fonctionner les systèmes d'information. À l'heure actuelle, cette réglementation est

---

* Par exemple Cornfield (Document no 3) ou Ryan (Document no 5)

ambiguë. C'est notre propos ici de proposer, comme objectif général, l'obtention d'une déclaration explicite sur la façon de recueillir l'information, la façon de la vérifier, la façon de la transmettre, c'est-à-dire à qui et dans quelles conditions, et ce, pour quelque système d'information que ce soit, public ou privé. Cet objectif s'applique même à un système d'information de police ou de sécurité.*

C'est délibérément que nous parlons surtout dans ce papier de système d'information au lieu de banque de données. Bien que les banques de données informatisées soient appelées à devenir de plus en plus nombreuses, il n'en reste pas moins que la grande partie des informations concernant les individus se trouvent encore rassemblées de façon conventionnelle sur fiches ou cartes poinçonnées. La tendance vers les circuits montés sur ruban magnétique, ou sur disque magnétique pouvant se relier à l'ordinateur, continuera sans doute pour des années à venir. Mais pour qu'une réglementation soit efficace, elle doit s'appliquer à la fois au présent et à la période de transition. Une réglementation doit être établie pour tout système d'information contenant des données sur des individus et non simplement pour des

---

* On doit faire une exception dans le cas (rare, espérons-le) de systèmes dont l'existence ne peut être divulgée pour cause de sécurité nationale.

...ques de données informatisées. Étant donné qu'un système contenant des informations sur une personne peut prendre un très grand nombre de formes, depuis l'annuaire téléphonique jusqu'au dossier de sécurité, il est nécessaire d'identifier les systèmes pour lesquels une réglementation s'impose.

...ification des systèmes d'information

Nous proposons ici de classifier les systèmes d'information contenant des données sur des individus suivant trois caractéristiques, chacune comprenant deux ou trois catégories. Ces caractéristiques et catégories apparaissent au tableau 1.

Tableau 1.

Caractéristique	Catégorie
Provenance de l'information	P - public record/document public
	S - supplied by individual/rapport de l'individu
	O - other/autre
Transfert de l'information	I - internal/interne
	E - external/externe
Inspection	A - automatic/automatique
	R - upon request of individual/sur demande de l'individu
	F - forbidden/défendue

Même si les expressions désignant les catégories donnent une idée générale de leur sens, nous devons en fournir des définitions précises.

Provenance de l'information: ce terme est clair quand l'information est rapportée par l'individu lui-même. Et comme "autre" se définit par exclusion des deux autres catégories, il reste donc à préciser le sens de document public. Pour ce faire, l'on pourrait dresser une liste de sources d'information acceptables, comme, par exemple, les certificats de civisme, l'immatriculation des véhicules, les rapports de condamnations judiciaires, les listes électorales, etc. Cette liste devrait être établie avec grand soin et révisée quant à son bien-fondé après un certain temps, mais son choix ne paraît pas présenter de difficultés insurmontables.

Inspection: la catégorie "automatique" veut dire qu'un rapport complet de données concernant un individu lui est envoyé à certains moments précis, soit périodiquement, par exemple, ou quand un changement est enregistré. Dans la catégorie "sur demande", il y aurait peut-être lieu d'imposer une légère rétribution pour transmettre à l'individu son rapport, de façon à décourager les demandes inutiles, mais autrment il ne semble pas s'imposer aucune autre condition. En particulier, l'individu doit avoir droit de voir

son dossier complet (autrement la catégorie devient "défendue") et ne doit pas être forcé de signer des formules l'empêchant d'intenter des poursuites en dommages qui pourraient résulter du mauvais fonctionnement du système d'information.

Les catégories les plus difficiles à définir sont "internes" et "externes" dans le cadre de la caractéristique "transfert de l'information". En général, interne veut dire que le transfert des informations est limité à l'entreprise ou à l'institution qui possède le système d'information, à moins que l'individu que touchent ces renseignements ne donne pas la permission explicite de les transmettre ailleurs, et ce, à chaque fois que le cas se produit. Cependant, quand il s'agit du gouvernment, fédéral ou provincial, il est évident qu'il faille conférer au terme "interne" des acceptions plus étroites en raison des vastes réseaux que forment ces organismes. Peut-être interne pourrait-il signifier un simple ministère ou bureau. Dans le cas d'une entreprise, il faudrait décider si ses diverses filiales seront considérées internes; même dans le cas d'une université, il resterait à savoir si certaines facultés et écoles seraient considérées comme appartenant au cadre interne de l'institution. S'il s'avérait impossible de définir le transfert interne avec assez de précision, il serait peut-être nécessaire alors de définir le transfert en fonction de données déterminées

plutôt qu'en fonction de tout le système. Nous examinons plus loin cette possibilité, mais pour le moment nous regardons les catégories "interne" et "externe" comme significatives.

En se basant sur ce système, nous indiquons au Tableau 2 un certain nombre de systèmes d'information courants et leurs classifications. L'on notera que quatorze des dix-huit types de systèmes possibles s'y trouvent. C'est dire que la classification par types est utile. La plupart de ces systèmes sont employés depuis longtemps et ont donné lieu à des méthodes de fonctionnement qui réduisent au minimum les problèmes de la vérification et de l'accessibilité. De fait, il ne se présente pas des difficultés que pour les types OEF et SEF. La réglementation des systèmes d'information pourrait donc procéder tout d'abord par l'identification des systèmes de types OEF et SEF. Pour tous les autres, et ils comprennent la très grande majorité des systèmes en usage: fiches de salaires d'une entreprise, annuaires de notabilités, morgues de journaux, etc., aucune réglementation ne s'imposerait pas. Cette façon de procéder encouragerait ceux qui maintiennent de tels systèmes à permettre à l'individu d'examiner l'information qui le regarde, et à en empêcher la divulgation générale, afin de la soustraire à toute réglementation. Là où il est jugé essentiel de permettre le transfert de documents, comme,

Tableau 2

Classification de certains systèmes d'information

Système	Type
Compte de banque	OEA
Feuille de paie	OIR
Annuaire de notabilités	SEA
Rapport médical	OIF
Dossier personnel	OIF
Casier judiciaire	OEF
État de crédit	OER
Dossier fiscal	OIF
Annuaire téléphonique	PEA
Liste électorale	PEA
Liste des ventes perspectives	PIF, OIF
Liste des ventes perspectives offerte en vente	PEF, OEF
Liste de membres (club, société prof.)	SIA, SIR SEA, SER (si donnée à l'autres)
Morgues de journaux	OER, OEF
Archives de la cour	PER
Liste d'assistance-sociale	OER or OEF
Livre de recensement	SIF
Fiches biographiques d'une entreprise	OEA

par exemple, entre deux corps de police de juridictions différentes, ou qu'il est jugé indésirable pour une personne d'avoir continuellement accès à son dossier complet, comme dans le cas d'un rapport médical, les conditions de divulgation ou de non-divulgation devraient être précisées. Je le répète, le but essentiel de la classification est de soumettre à un contrôle quelconque tout système d'information où se posent des problèmes de sécurité et de divulgation, et non seulement les banques de données informatisées.

Bien que cette classification puisse suffire à réglementer les systèmes d'information, en pratique il faudrait établir des distinctions beaucoup plus précises sur les catégories de données. La question la plus difficile à se poser restera toujours: à qui doit revenir l'autorité de recevoir telles out telles données? On ne peut attacher trop d'importance à cette question. À la longue, il faudra avoir recours à l'emploi systématique d'indices de sécurité reliées à chaque champ de données, pour déterminer dans quelles conditions l'information pertinente peut être divulguée. Dans les cas ordinaires, le code d'autorisation de l'usager peut suffire à cette fin; dans les cas plus compliqués, il peut être nécessaire de dresser une table reliant les codes d'autorisation aux indices.* L'emploi

---

* Le manuel de l'IBM "The Considerations of Data Security in a Computer Environment" touche à la question des techniques et tables d'autorisation à la page 16. Voir aussi Ware et al.: Spring Joint Computer Conference, 1967, pp. 279-303.

d'indices de sécurité entraîne des coûts supplémentaires dont nous parlerons plus loin. Mais à mon avis, il importe de reconnaître que ces coûts sont nécessaire et qu'un tel circuit doit inévitablement faire partie intégrante de tout système d'information. Toutefois, vu la rareté de ces systèmes, notre manque d'expérience en ce domaine et le fait qu'ils ne puissent être ajoutés aux systèmes existants que sur une période considérable de temps, il n'est pas pratique d'inclure dans la réglementation proposée l'adoption obligatoire de fiches de sécurité informatisées.

4. Coûts

La réglementation des systèmes d'information suscite trois sortes de coûts: directs, indirects et prohibitifs, ces derniers attribuables aux restrictions rendant impossible l'exercice de certaines activités.

Outre les sommes nécessaires au maintien d'agences de réglementation et d'octroi de licences, les coûts directs comprennent l'achat de brouilleurs et autres dispositifs de hardware destinés à protéger les informations, déceler les dérivations possibles sur les canalisations, etc. Hoffman (document no 1) étudie cette question plus en détail. Il est certain que l'usage de ces mécanismes se répandra si une législation de protection de l'information est mise en vigueur.

Les coûts indirects résultent de la nécessité de maintenir des systèmes de software plus complexes. Il faut compter les frais encourus dans la transmission de copies de données disponibles aux individus, soit automatiquement soit sur demande ou simplement par la classification de divers champs de données et les indices auxquels ils correspondent. Il sera peut-être opportun de prendre des précautions pour que cette tâche ne finisse pas par s'entourer de toute une mystique, comme c'est le cas, dit-on, de l'information classifiée pour raison de sécurité militaire. Il faut compter aussi le coût de stockage des indices et le temps consacré au déchiffrement des codes d'autorisation et au retracement de l'indice connexe. Notons en passant qu'il existe déjà des systèmes d'information où plusieurs données sont répétées sous forme d'indices reliés à des champs d'information. Dans le système Marc II, de plus en plus adopté pour l'information bibliographique, environ 10% du stockage est affecté aux indices qui permettent d'identifier les données, faciliter l'accès et le comptage, etc. Si ce genre de stockage et de services supplémentaires se trouvent dans un système d'information bibliographique, il n'y a aucune raison pour qu'ils ne soient montés aussi dans les systèmes d'information concernant les individus.

Les coûts prohibitifs surviennent quand il devient difficile ou même impossible de mettre à exécution certains

projets méritoires, tels certains travaux de recherches ou études de sciences sociales, si l'accès à l'information privée fait l'objet de sérieuses restrictions. Mais nous avons l'habitude de ces obstacles dans les domaines de l'expérimentation médicale et psychologique sur des êtres humains, où les limites juridiques sont définies avec soin, et nous en acceptons la nécessité. Il faudra de même accepter la nécessité de coûts dits "prohibitifs" dans le domaine de l'informatique.

5. Propositions

En guise de conclusion, nous formulons trois propositions que nous croyons exécutables et dont l'adoption aura un effet appréciable sur la préservation du droit à la vie privée.

1) Le concept juridique de la transgression du droit à la vie privée doit être défini dans la loi canadienne.

Ce concept doit aller plus loin que les termes des présentes lois sur le droit au secret concernant avocats, médecins, banquiers, employés, époux. La loi doit s'étendre aux tables d'écoute (wiretapping)[1], aux bureaux de crédit[2], aux systèmes d'informations médicales[3], et aux autres types de systèmes d'information.

---

1 Cornfield, document no. 3
2 Gibson & Sharp, document no. 2
3 J.C. Ogilvie "Legal and Related Problems of a Health Information System"

2) Certains types de systèmes d'information doivent détenir une licence.

Ici, la législation peut suivre les grandes lignes proposées dan "Computers and Freedom"[4], le Bill 182[5], et "Privacy and Commercial Reporting Agencies"[6]. La licence d'exploitation doit s'appliquer aux systèmes d'information et non seulement aux banques de données et se baser sur une classification qui catégorise les systèmes suivant leur mode de fonctionnement. La transition vers les systèmes d'information établis par ordinateurs devrait simplifier la mise en vigueur des contrôles.

3) Les innovations techniques susceptibles de permettre une sécurité et un contrôle plus grands sur le transfert des informations doivent être encouragées.

Nous avons besoin tout particulèrement de techniques efficaces pour relier données pertinentes et usagers autorisés; nous avons aussi grand besoin de hardware peu coûteux capable d'assurer le maintien de la sécurité. L'encouragement ci-devant mentionné peut prendre la forme de subventions pour certains projets, d'avantages matériels offerts aux manufacturiers et compagnies de software pour

---

4 NCP Old Queen Street Paper: 8, Conservative Research Department 1968

5 An Act to Provide for Data Surveillance, 2nd Session 28th Legislature, Ontario 1968-69

6 Document no. 2, p. 31

mettre au point et commercialiser des systèmes et pour faire connaître les méthodes et appareils déjà inventés. Analystes et concepteurs de systèmes, il va sans dire, devraient se servir de l'outillage présentement disponible.

L'homme est en train d'apprendre que les effets de la technologie no sont pas tous désirables. La question de la pollution, qui nous préoccupe tant en ce moment, n'est qu'un des aspects d'une vaste revue qu'il faut entreprendre sur les effets secondaires de la technologie. Les cas les plus sérieux sont ceux où il est impossible de renverser l'ordre des choses. Ainsi, un lac pollué constitue un problème bien plus grave qu'une rivière polluée. En informatique je ne suis pas d'opinion que nous approchons rapidement du phénomène d'irréversibilité. Mais il est intéressant de constater que chaque examen des effets de la pollution et de la radiation produit un abaissement des niveaux de tolérance permis. Il est possible que l'introduction de mesures de réglementation des systèmes d'information n'exige pas un prix inutilement élevé au début, mais la prudence demande que nous agissions tout de suite. L'expérience démontre que la surprotection des droits est très rare. À mon avis, si la question de la protection du droit à la vie privée est bien expliquée au public et aux autorités politiques et juridiques, si toutes les conséquences en sont bien démontrées, nous réussirons à

convaincre les intéressés à faire leur part pour assurer le bon équilibre de notre environnement social. De fait, ils insisteront probablement pour participer à cette noble tâche.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 4

Regulations for Information Systems

Goals, Means and Costs

by

Calvin C. Gotlieb

University of Toronto

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

REGULATIONS FOR INFORMATION SYSTEMS
GOALS, MEANS AND COSTS

by

Calvin C. Gotlieb
University of Toronto

A paper prepared for the conference "Computers: Privacy and Freedom of Information to be held at Queen's University

Kingston, Ontario
May 21 - 24, 1970

RESUMÉ

A classification of information systems is proposed which could help in identifying systems where there are problems of security and disclosure of information. Costs arising out of regulation are examined, including direct costs for hardware, indirect costs for the more complicated software which would be needed, and inhibition costs because certain types of activities would be restricted. It is concluded that: in spite of the problems and costs associated with regulation, a legal concept of privacy should be introduced in Canadian law; certain types of information systems should be licensed; and technical improvements which would permit greater security and control over the transference of information should be encouraged.

Regulations for Information Systems
Goals, Means and Costs

by

Calvin C. Gotlieb
University of Toronto

1. Background and Viewpoint

The six papers distributed to participants give the background to the dilemma posed in the title to this conference. Briefly, the argument proceeds as follows:

(i) Information Systems are Increasingly Necessary

Information systems containing data about individuals are needed increasingly in the public sector (census data, tax records, medical statistics, police fields, etc.) and in the private sector (records for banking, credit, insurance, etc.). Governments need these records to carry out their responsibilities; planners and social scientists need them to understand our society and suggest measures to take it in the directions considered desirable; business needs the records for effective operations, service and management.

(ii) The Trend is to Integrated Systems

There is a strong trend towards integrated systems -- i.e. systems that contain heterogenous information about many people and which are accessible to different authorities for different purposes. The ability to gather more accurate and consistent data, and the advantages of lower costs and better coverage, make such systems irresistible.

(iii) Our Laws Offer Poor Protection Against Misuse of Information

The concept of privacy is very poorly defined in Canadian law. Rules governing which agency may collect what information, how data should be verified and to whom it may be disclosed, exist in only a few situations. As a result the individual is not protected against the misuse of information about him.

(iv) The Trend to Computerized Systems Increases the Dangers

Technological advances in storage and communications devices are leading to integrated information systems built around computerized data banks. Availability of terminals and ease of communications increase the danger that data about a person may be distributed without restriction and used for purposes detrimental to his interests. The dangers are often aggravated by an unjustified confidence in data coming from a computer.

(v) Proposals to Regulate Data Banks are Controversial

This chain of reasoning leads to proposals for regulating data banks, e.g. by licensing them; various such proposals have been presented in the background papers and are being put forward at this conference. Opponents of regulations argue that they are in general addressed to the wrong problem and in any case unenforceable. Proponents argue that it is essential to adopt firm measures before there is an irretrievable loss of human rights.

It is accepted in this paper that some regulation of information systems is required. No new arguments for regulation are advanced. Most people attending this conference have probably formed opinions on whether privacy is really being eroded and these are not likely to change as a result of the conference. In my opinion the crucial question is: can effective regulations be formulated and enforced? Many of the arguments against regulation are based on the view that information systems are too thoroughly woven into the fabric of our technology to be limited, that any regulation which would protect privacy would exact unacceptable costs in loss of efficiency and opportunities, and that some diminution of privacy is unavoidable. This vew is not accepted here. This paper is an attempt to examine goals and to show that adopting measures to achieve them is not impossibly difficult.

2. Goals

It is not difficult to list goals which are almost truisms. For example:

- The rights of an individual to privacy must be protected as much as possible, consistent with the legitimate needs of society.
- Data concerning individuals must be as accurate as possible.

The problems arise when it is necessary to interpret the meanings of specific phrases such as "individual rights", and "legitimate needs of society", in knowing when reasonable steps to provide protection or ensure accuracy are being proposed.

The first proposition above implies a middle position in privacy vs. freedom of information. It suggests that a person cannot expect to opt out of society by refusing to recognize that some records must be kept about him - e.g. birth registration and social security number. But it does assume that there are rights of privacy for an individual. Since it is generally agreed* that the legal concept of privacy is poorly defined in Canadian law if at all, it follows that there must be legislation to define individual privacy. This is an essential point. If I do not dwell on it further in this paper, it is because I do not regard myself qualified to discuss where in Canadian law such legislation ought to reside - whether as Ryan suggests it should exist in a provincial law or in federal, or both, and in which sections of the law it would be most appropriate. I hope

---

* See for example Cornfield in background paper No. 3, or Ryan in background paper No.5

that during the course of this conference specific propsals for legislation will emerge.

A legal concept of privacy, though necessary, is not enough. It is also necessary to consider how the concept should interpreted when operating information systems. In particular it is important to relate the concept to the rules which those who are responsible for designing, assembling and maintaining information systems, are to use in handling data. At present these rules are ambiguous. It will be taken as a general goal here that it is desirable to have an explicit statement of how information is collected, how it is verified and to whom and under what conditions it is transmitted, for any information system, public or private. This is desirable even for a police or security information system.*

In this paper the emphasis on the phrase information system, rather than data bank, is deliberate. Although computerized data banks are coming to the fore, most of the data about individuals is still in the conventional form of files or punched cards. The transition toward systems stored on magnetic tapes, or on magnetic disks which may be attached on-line to a computer, will undoubtedly continue

---

* An exception must be admitted for those (hopefully rare) systems, for which because of national security, the existence is not made known.

for decades. But to make any regulation effective it must be applicable both now and through the transition period. Regulations must be considered for any information system which contains data about individuals, and not simply for computerized data banks. Since a system which contains information about a person may take a wide variety of forms, ranging from a telephone book to a security file, it is necessary to identify those systems for which regulation might be needed.

3. A Classification of Information Systems

It is proposed here to classify information systems containing data about individuals according to three characteristics, each with two or three categories. The characteristics and categories are shown in Table 1.

Table 1.

Characteristic	Category
Data Source	P - public record
	S - supplied by individual
	O - other
Distribution	I - internal
	E - external
Inspection	A - automatic
	R - upon request of individual
	F - forbidden

Although the terms used for the categories convey a general sense of their meaning, precise definitions have to be given.

For Data Source it is clear enough when the data is supplied by the individual himself, and since "other" is defined by exclusion, the definition hinges on what is meant by public record. This could be defined by listing those sources which were acceptable - e.g. public service awards, vehicle registrations, records of criminal convictions, voters' lists, et. Careful thought would be needed to choose the list and it would have to be reviewed in the light of experience, but there does not seem to be any inherent problem in arriving at a definition.

For Inspection the "automatic" category means that a complete print-out of the information about an individual is sent to him at specified points - e.g. periodically or whenever a change is entered. In the "request" category there might conceivably be some small fee charged if a person wishes to see his print-out, so as to discourage nuisance requests, but there should be no other condition imposed. In particular an individual must be allowed to see the whole record (otherwise the category should be "forbidden"), and he should not be required to sign forms which prohibit him from presenting

claims for damages arising out of improper operation of the information system.

The most difficult categories to define are "internal" and "external", with respect to the Distribution characteristic. 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. Perhaps internal should mean a single department or office. For a company, a decision would have to be made whether various subsidiaries were to be considered internal, and even for a university the question arises whether different faculties and schools are all to be considered as internal to the one institution. 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 system. This possibility is discussed at greater length below, but for the moment it is assumed that the categories "internal" and "external" are meaningful.

Using this system a number of common information systems are shown in Table 2., along with their classification. It will be observed that fourteen of the eighteen possible types occur in this table. This is some evidence that the classification into types is useful. Most of these information systems have a long history of use, and methods for operating them have evolved to minimize problems of verification and accessability. In fact problems really arise only for the types OEF and SEF. Regulation of information systems could therefore proceed by first identifying those of type OEF and SEF. For all others, and this would include the overwhelming majority of systems - company payroll files, who's who, newspaper morgues, etc. - 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. Where it is judged essential to permit the transfer of records - e.g. between one law enforcement jurisdiction and another, or it is judged not desirable for a person always to have access to his complete record, as might be the case with a doctor's report, the conditions for allowing disclosure or preserving security would be spelled out. I repeat that the essential purpose of the classification is to allow attention to be

Table 2.

Classification of Some Information Systems

System	Type
Bank Account	OEA
Payroll File	OIR
Who's Who	SEA
Medical Report	OIF
Personnel File	OIF
Police File	OEF
Credit Record	OER
Tax File	OIF
Telephone Book	PEA
Voters List	PEA
Sales Prospects' File	PIF, OIF
Sales Prospects' File for Sale	PEF, OEF
Membership List (Club, prof.society)	SIA, SIR
	SEA, SER (if given to others)
Newspaper Morgue	OER, OEF
Court Records	PER
Welfare List	OER or OEF
Census Record	SIF
Biographical File of Company	OEA

focussed on any information system where there are problems of security and disclosure, and not just on computerized data banks.

Although this classification system could be adequate for setting up regulations about information systems, in actual operation it will probably be desirable to make much finer distinctions about categories of data. The most difficult question will continue to be: who should have authority to receive specified items of data? It is impossible to take a simplistic approach on this. Eventually the only satisfactory solution will be to attach security tags to every data field, and use these tags to determine under what conditions the information may be disseminated. In simple cases the user's authorization code may be sufficient to determine which fields are available to him; in more complicated situations it may be necessary to set up a table which relates authorization codes to tags.* There are define overhead costs associated with security tags and these are discussed further below. In my opinion it will come to be recognized that these costs must be paid and a security tag system will be a normal feature of every information system. But

---

* The IBM manual "The Considerations of Data Security in a Computer Environment" discusses, briefly, authorization techniques and tables (p.16). See also Ware et al.: Spring Joint Computer Conference, 1967, pp. 279-303.

the lack of experience with such systems, and the fact that they are so far rare and would have to be added to existing systems over a considerable period does not make it practical to suggest that proposed regulations on information systems make it necessary to include security tags for data.

4. Costs

Three types of costs will be associated with the regulation of information systems: direct and overhead costs, and inhibition costs arising from things which cannot be done.

It will obviously take funds to maintain regulatory and licensing agencies. Other direct costs to be paid by the purchaser of hardware will be for scramblers, and other devices for protecting information, detecting possible taps on the communication channels, etc. Hoffman (background paper no. 1) discusses these in some detail; they would certainly come into wider use if the operators of information systems are made to take on legal responsibilities for safeguarding data.

Overhead costs would arise from the more complicated software systems which would be needed. There would be costs in making transcripts of data available to individuals either automatically or on request or simply in classifying

different data fields and assigning tags to them; care might have to be taken that this task was not expanded to the point where it had a whole mystique attached to it, as is said to be the case with data classified for military security. There would be costs for storing tags and the time taken to decode authorization numbers and match them against tags. On this latter point it should be noted that there are already information systems in which a deal of redundant information is carried in the form of tags attached to data fields. In the Marc II system now being adopted widely for bibliographic information perhaps 10% of the storage is used for tags that identify data, facilitate access and counting etc. If this type of storage and processing overhead can be built into a system for handling bibliographic information, it is not too much to expect that it will also be built into systems for handling personal data.

There would be inhibition costs because worthwhile activities would be more costly or forbidden. It would be more difficult or even impossible to carry out certain types of planning studies and experiments in the social sciences if access to personal data became more restricted. But we are used to such inhibitions in medical and psychological experimentation involving human beings, where there are very careful legal and other regulations about what

may be done, and we accept the necessity for them. We will have to accept similar inhibition costs when using personal information.

5. Proposals

This paper concludes with three specific proposals which, it is believed, are capable of implementation, and will have significant effects on the preservation of individual privacy if adopted.

1) A legal concept of the invasion of privacy should be introduced in Canadian law.

This should go beyond the present laws on non-disclosure governing lawyers, physicians, bankers, employees, spouses. It should be broad enough to be applicable to situations involving wiretapping[1], credit bureaus[2], health information systems[3], and other types of information systems.

2) Certain types of information systems should be licensed.

Legislation could follow the general line suggested in Computers and Freedom[4], Bill 182[5], and Privacy and Commercial Reporting Agencies[6]. The licensing should be

---

1 Cornfield, background paper no. 3
2 Gibson and Sharp, background paper no. 2
3 J.C. Ogilvie "Legal and Related Problems of a Health Information System"
4 NCP Old Queen Street Paper: 8, Conservative Research Department 1968
5 An Act to Provide for Data Surveillance, 2nd Session 28th Legislature, Ontario 1968-69
6 Background paper no. 2, p. 31

for information systems and not merely data banks, and be based on a classification which categorizes systems according to their mode of operation. The transition to computerized information systems should simplify the application of controls.

3) Technical improvements which permit greater security and control over the transference of information should be encouraged.

Particularly needed are effective techniques for matching data with authorized users, and inexpensive hardware for maintaining security. The encouragement could take the form of research grants on projects, incentives to manufacturers and software companies to develop and market systems, and publicize the methods and devices already known. Systems analysts and designers should use the tools presently available.

Man is learning that not all the effects of technology are beneficial. Our concern over pollution is only one aspect of the review which has to be undertaken about many side-effects of technology. Especially serious are those cases where the processes are almost impossible to reverse. A polluted lake is a much greater problem than a polluted river. I do not feel that we are far along an irreversible process in the way we are allowing

information systems to operate now. But it is noteworthy that every review of the tolerance for pollution or radiation leads to a downward revision of the permitted levels. I feel that it is possible that introducing regulation and licensing for information systems might exact a price which is unnecessarily high at first, but I prefer to see caution on the side of protecting rights. Experience has shown that overprotection is in fact, very rare. In my opinion if the problems regarding protection of individual privacy are explained to the public, and to those responsible for political and legislative action, and the alternatives are set out, they will be willing to pay the price of keeping our social environment healthy. In fact they may well <u>insist</u> that the price be paid.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 4

Computers and Society

by C. C. Gotlieb F.R.S.C.

a paper presented to The Royal Society of Canada, June 1969

*****

DOCUMENT NO 4

Computers and Society

par C. C. Gotlieb F.R.S.C.

une conférence prononcée devant les membres de

La Société royale du Canada, juin 1969

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

Science and Society - New Concerns

An examination of computers in society today must be placed in the context of the larger topic, "Science and Society". The belief in the separation of science and the state, which most of us probably cherished in our student days, was given its first serious challenge with the dropping of the atomic bomb. "The Bulletin of The Atomic Scientists" published by scientists who made the bomb, reflected their concern in the new political and moral issues which had arisen from their actions. Concern about the effects of science on society has grown steadily in the last 25 years. Now there are a dozen issues being debated with feverish intensity - a debate which is taking place in many forums - at scientific meetings, on radio and television as found in the excellent CBC series, "Science and Conscience"*, and in interdisciplinary seminars, such as that on "Science and Society" recently sponsored by the University of Toronto School of Social Work. It is no exaggeration to say that, science and scientists are on the defensive. Scientists are being challenged for the role they play in helping to produce nuclear weapons, anti-ballistic missiles, electronic defense systems and the weapons of biological warfare. The challenge comes mainly from the younger,

*A Television Symposium, Canadian Broadcasting Corporation, 1969

activist sutdent and faculty in our universities, but it is being pressed vigorously, and it is not possible to say at this moment what it will lead to. And, even those scientists who are not engaged in "offensive disciplines", for example, astronomers and geologists, are blamed for sins of ommission. Some years ago, Jacques Barzun wrote, "Science - the Glorious Entertainment",* in which he accused scientists of indulging in an amusing pasttime, without paying regard to the needs of society and humanity. More specifically, scientists are now being urged to direct their energies to useful missions - to reduce pollutions, to help rebuild our cities, and to help plan our social systems so that more consideration is given to man as an individual. It is in this context then, that I turn toward the subject of "Computers and Society".

Fears About Computers

The ambivalence that one hears expressed about the benefits of science has been present almost from their beginnings, about computers. In 1958, Norbert Wiener in his book, "The Human Use of Human Beings",** expressed his

* Harper and Row, 1964.

** Houghton & Mifflin Co., Boston, 1958

fear that computers would bring about wholesale unemployment, and his hope that they would be brought into use wisely, without indicating how that wisdom might be exercised. Since then, the growing use of computers has obviously worried a great many people, as shown in wry cartoons, in public discussions, and in the numerous articles on the social implications of computers.* The destruction of the computer centre at Sir George Williams University last December (and the occupation of the computer centre at McGill by separatists which preceded that event) seems to have been sparked by the desire to sieze a hostage, but undoubtedly behind this desire lay the students' fear of an inhuman machine which seemed to direct their lives.

In thinking about those aspects of computers which make people uneasy, and in discussing them with different groups, I believe I can identify at least five areas of concern:

1) the fear that computers will cause widespread unemployment,
2) the fear that man is being rendered obsolete by an intelligent, infallible, device,

* See for example, the bibliography by Michael A. Duggan, "Computer Utilities, Social and Policy Implications", Computing Reviews, October 1968.

3) the fear that computers are depersonalizing our society, turning people into numbers,

4) a fear that computers are propelling us towards a society run by "technocrats", where important decisions are made every day by persons of narrow viewpoint who are insensitive to social and humanistic factors or, the ultimate horror, are made by unfeeling robots.

5) a fear that computers, especially through the data banks, which they make possible, will bring about an irretrievable loss of individual privacy.

These items are obviously not altogether distinct - the first two are related, as are the last three, and they do not express all the suspicions which people have about computers. But they are fears which are often voiced, and I would like to address myself to each of them. Let me anticipate my conclusions by saying I believe that a careful examination of the facts shows that in the first three cases, there do not seem to be permanent threats, but that on the last point we will probably need concerted action to bring about legislation to protect people against the loss of cherished liberties.

Computers and Unemployment

Wiener who first raised this issue drew heavily upon the history of the industrial revolution in his argument. But we have now had more than a decade to observe the effects of computers on unemployment, and I believe that the problem is being contained. Certainly there are places where the introduction of computers has suddenly made specialized skills obsolete - witness for example the effect of computerized typesetting on newspaper linotypesetters. Computers, however, present only one important facet of the changes resulting from automation. Serious dislocations do arise and they have to be met by a variety of responses - retraining programs, guaranteed annual wages, regional programs for aiding industry, and a general approach which protects the person rather than the job. But in developed countries at least, the growth of the economy, to which automation and computers contribute significantly, seems to be providing jobs in increasing numbers, even to meet our increasing population. Data on this important question is difficult to interpret (see for example the reports, Labour and Automation*), but a significant factor is the very heavy requirement for

* Labour and Automation, Bulletins 1-5, International Labour Office, Lausanne, Switzerland 1964-1968.

people in the data processing industry itself. To repeat then, the evidence is that the effect of computers on unemployment presents a problem which is containable.

Infallible Intelligences

If you examine the details of a computer program which exhibits artificial intelligence you are bound to wonder why the term intelligence is associated with such an uninspired effort. For example, in a well-known checkers-playing program the best move is calculated from a linear function with weight factors multiplying quantities representing the parameters of a position--material advantage, tempo, mobility, etc. The so-called learning the program exhibits is simply a determination of the weighting factors based on the history of play.

The point I am trying to make here is that to the initiated, computers do not possess anything which corresponds even remotely to an intuitive concept of intelligence. Yet there seems to be a powerful fear of intelligent machines--- a fear found in persons who are highly educated as well as those with little formal education. We have not explored the limit of what we can do with computers, but we have come to recognize that there are definite limitations to what we can expect from them in the foreseeable future. There has been a definite retreat with respect to language translation by computers, and we have no idea how to make a machine develop abstract concepts. Although the question of machine intelligence

is one of the more interesting speculations about computers, fears of a superintelligent device do not stand up against rational examination.

When we come to machine infallibility we find a similar pride in what has been accomplished and relief in the presence of weakness. People welcome the automation which relieves them of repetitive labour, and seize on instances of machine fallibility, as can be seen in the gleeful newspaper reports about a computer which has stupidly printed a cheque for a million dollars. Here again the fears seem foolish when they are brought out into the open.

Nevertheless these fears about a too-perfect device are very deep-rooted. I suspect that the whole syndrome is an aspect of man's search for perfection and his worry that one day he might just find it.

Computers as Agents of Depersonalization

Many of us who work with computers regard it as ironic that computers should be blamed as the instruments which reduce us to numbers and holes in a punched card, when we feel the facts are that computers offer the best chance of retaining our individuality in the midst of a society which has to deal with masses. Perhaps the resentment that people bear towards computerized systems comes about because of the frustrations we have all experienced in trying to deal with a faulty automatic system, as is all too often found in a computerized billing operation or in a disembodied telephone voice. Before adopting a luddite view of these manifestations, it must be recognized that the real problems arise from the increasing population of the world, and from the authoritarianism which characterizes many governments. Perhaps the best known representation of a fictional, depersonalized society is that in Orwell's 1984, and this, it will be recalled, was achieved without the aid of com computers. Again, many regard China as the extreme example of an actual depersonalized society, and here too computers play little role.

Whatever hope we have of retaining our individualism in today's population explosion may well lie in having computers keep track of our personal

preferences and individual characteristics. When we order a new car today, for example, it is possible to have a model assembled with the color, style, and extra features we select, ready for us within a few weeks. Whatever we may think about such preferences as a value in our society, we must accept that people want to choose, and this kind of choice is possible because computers have been incorporated into the production assembly system for automobiles. Coming to a more important case, we can foresee the time when each of our complete, individual medical histories will be available to doctors and hospitals when necessary, and there is little doubt that having the comprehensive medical file on a patient will confer important advantages in treatment. Or turning to the accessibility of scientific information, some of you may already be using one of the selective dissemination information services which offer to an individual scientist, regular listings of all articles which meet his personal interest profile. As a final example I would point out to you how efficient our airline reservation systems have become in a remarkably short time, and how easy it is for a ticket agent to identify you if you wish to change a routing or make a stop-over.

There is a caveat in having our personal choices so well looked after. If computers can keep track of our

individual preferences so meticulously, they can be also used to compile dossiers on us, a possibility repugnant to those brought up in a system based on British justice. This prospect is not to be dismissed lightly, and I shall return to it in discussing data banks. However, it remains true that computers will be able to deal with our preferences, record our individual characteristics where it is important that these be available on short notice, and in many many ways, help a society, which is becoming increasingly service-oriented, to cater to the wishes of the individual. Although we have an increasing use of postal zone districts, social insurance numbers, and account identification numbers, this proliferation does not mean that people are being reduced to numbers. The important question is whether we can receive individual attention, and I maintain that our computer-based service systems will make this possible in an increasing variety of situations.

A Society Run By Technocrats

This threat is a general one posed by the growing specialization in our society. Once again it cannot be dismissed lightly, but the problem presented by computers must be regarded as one facet of the general problem. Are our legal freedoms impaired because the law has become so complex that we have to choose a lawyer who is an expert

on our problem? Is our health jeopardized because medicine has become so sophisticated that a general practitioner and perhaps several specialists are needed for almost any diagnosis and cure? Somehow it seems that we have to find a way to survive in our society even though we must keep calling upon authoritative help in more and more situations. The only solution seems to be that our general education must contain enough information about these specialities so that a lay person can know who to turn to for advice, and perhaps be prepared to make personal judgements about those factors which concern him vitally. We must rely on the competence of specialists, and yet we must know enough about say, law or medicine, to be able to come to some opinion about a lawyer or a doctor when it is a matter of supreme importance to us. I feel that the situation with regard to computer specialists is very much the same. Our whole education system will have to contain at least the elements of training and knowledge about computers and programming, about their effects upon society, and about the mechanics of computer operation, so that as lay persons, as accountants, or scientists, or social workers, we understand enough about such things that we are not at the mercy of the expert practitioners. This seems to be difficult to achieve, but it is a challenge to our educational system, and one which must be met.

Data Banks - Privacy and Security

I come now to the question of data banks and the threats these pose to individual privacy. There already are in existence many separate files about any of us. Our medical histories are on file in doctors' offices, hospitals and insurance companies; statistics on our income are on file in the tax department and in the social insurance department; a file on our travel history exists in the external affairs passport department. And most certainly our bank and one or other of the commercial agencies which provide credit ratings maintain a credit file on us. What is now possible is that all of these separate files can be pooled to make a very complete picture which would have a great many details we regard as private matters. Some of you may be aware of the massive hearings which have taken place over the last four years in the United States House of Representatives and in the Senate, on computer privacy. What has emerged from these is that while it is relatively easy to store vast arrays of data, it is much harder to ensure quality control. What is even worse, is that there are almost no legal safeguards to prevent files on us from being used without our knowledge, and in ways which could be damaging. Salton* points out how files are used for purposes quite different

* G. Salton "On the Future of Mechanized Information Files", Comm. acm, January 1968.

from those originally intended, in the widespread custom of buying and selling mailing lists, without informing or asking permission from the people whose names appear on the list.

Ramey, at the 1967 annual convention of the American Documentation Institute, made the following suggestions for ensuring privacy:

1) computer personnel dealing with mechanized information files should be licensed and/or bonded, and strict rules of professional privilege should apply to the file operations, in the same sense, that transactions between lawyer and client, or doctor and patient are now deemed to be privileged;
2) the transmission of identifiable personal information from one data bank to another should be prohibited without the express permission of the person whose data are to be transmitted;
3) a "writ of hard copy" should be obtainable by each individual whose personal information is stored in a mechanized information system;
4) a "writ of erasure", preceded if necessary by an advocacy hearing, should be obtainable by which personal information deemed to be misleading or inaccurate can be deleted from the file.

These proposals, if adopted, might go a long way towards protecting the individual from unfair exploitation of information about him. Unfortunately, if the usual route in developing legislation for the protection of the public is followed, it will require many years and many painful instances of injustice before laws are enacted.

Once consensus is reached about questions of privacy and fair use of information, there still remains the technical problem of achieving the security of files. Safeguards will have to be incorporated into data banks. These might include*:

1) Devices which would shut out anyone who does not identify himself by a password or by a badge which can be inserted into a terminal.
2) Cryptographic techniques which would protect information being transmitted from a computer to a distant terminal over telephone lines.
3) Techniques for recording every request for information, and for identifying the person who made the request.

Such devices are technically possible but it must be emphasized they are not present on any of the storage systems now being marketed.

* These are contained in an address, "Technology and Privacy" given by T. J. Watson, Jr. to the Commonwealth Club of California, April 1968.

Conclusion

You may feel that in this talk on Computers and Society I have been too much on the defensive. Computers are rightly regarded as a cutting edge of our technology. We expect computers to help us increase our productivity, solve our traffic problems, teach our youth, and in a thousand ways, to help us cope with our manmade complexity. And let me affirm that I am convinced that computers can indeed contribute to all of these. But I have chosen to concentrate on the dangers of computers - imagined and real. One of the ways in which responsible scientists must meet the challenge of those who are questioning science is to show that we are aware of both the benefits and dangers of the products we are developing. And, further, that we are prepared to participate in efforts which will keep the benefits, and minimize the dangers.

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 2

Data Banks for Credit Bureaus

by

The Associated Credit Bureaus of Canada

M.T. Pearson, General Manager

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

"Data Banks For Credit Bureaus"

Prepared By The
Associated Credit Bureaus of Canada
M. T. Pearson, General Manager

For The Conference On

"Computers: Privacy and
Freedom of Information"

Queen's University, Kingston, Ontario, Canada

May 21-24, 1970

SUMMARY

"Data Banks For Credit Bureaus"

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

Gentlemen,

You have read the Brief from the Associated Credit Bureaus of Canada on "Data Banks for Credit Bureaus".

We will not go into detail on the importance of credit and credit bureaus in today's economy. All studies and investigations of the industry carried out in Canada and the U.S. in the past 10 years agree that credit and the credit bureau industry play key roles in modern society, and contribute extensively to the high standard of living we enjoy today in North America.

We also will not discuss all the policies established by Credit Bureaus in Canada and the United States in recent years to protect the privacy of the individual. Policies on file content, access to files, service contracts and personnel reporting are given in detail in our Brief. They coincide with provisions of the United States Fair Credit Reporting Act which has now passed the United States Senate. In our opinion, theyprotect the consumer from unwarranted invasion of privacy now, and will continue to be effective in the future.

It is our opinion also that these safeguards and limitations on Credit Bureau activities will prevent any invasion of privacy as a result of computerization. Computerized Data Banks for Credit Bureaus, in short, will not change this situation and, in fact, may

assure increased privacy. This is so because

- firstly, file content is limited to a few essentials on which credit can be granted. This content will not be expanded to become a complete personal dossier because, as industry policy clearly states, only information on an individual's credit performance is kept.
- secondly, computer programs are already developed and operating in the United States with more built-in safeguards than manual systems now used in Canada.
- no Canadian credit reporting Bureau is presently computerized, nor have any announced plans to do so. We are confident, however, that when credit data banks are on computer, they will present no invasion of privacy problems.

You will note in the Brief the results of a 1968 survey of customer complaints to Canadian Credit Bureaus. Out of more than 4,200,000 reports, there were 370 cases of mistaken identity (all cleared up promptly) and 348 cases of error or other complaint. The latter is a complaint or error rate of 0.01%, or one per every 10,000 reports. It is interesting also to note that of 9,500 people who visited Bureaus for various reasons in 1968, nearly two-thirds, or 5,915 came to the Bureaus because they thought the Bureaus themselves had turned down their applications for credit.

"Charge it!" is a common term today. Every time you say this, a form of credit is implied - credit based on trust and confidence.

The vast majority of consumers accept credit bureaus and their services as a way of life. In fact, they want the convenience of easily available credit and are quite willing to be included in the data bank because they realize that credit is a privilege based on trust between two parties.

Computerized data banks supplying basic, factual information will, in our opinion, be welcomed by the public as a modern, efficient way to fill this need.

I N D E X

Index (cont'd)

INTRODUCTION

A great deal has been written and said about Invasion of Privacy in recent years. The complexity of the subject can be seen by the variety of definitions of what Invasion of Privacy means. One authority states that "the basic attribute of an effective right to privacy is the individual's ability to control the flow of information concerning or describing him". Another source defines it as the distribution of inaccurate or misleading information, or the unjustifiable use of information, for example, use in a way not intended when the information was originally made available. A third sees the threat as accidental or intentional disclosure of confidential data, or unauthorized modification of data. While it does not define invasion of privacy, the letter received by the Association requesting our participation in this conference states that "rules of conduct by all concerned must be established, and very quickly.....".

We conclude, from these varied opinions on what we are talking about, that simplification of the subject, as far as the operations of members of the ACB of C are concerned, is called for.

Our definition of invasion of privacy, therefore, is straightforward. We believe it can be measured by three questions:

1. Is the information considered confidential?
2. Is it used only for the purpose for which it was gathered?
3. Does the Consumer have an opportunity to refute it?

Our contention is that the operations of Credit Bureaus in Canada, now and in the foreseeable future, fulfill all three conditions above, and do not represent a threat to invasion of privacy.

The remainder of this Brief will attempt to substantiate this conclusion.

I THE ORIGINS OF CREDIT AND CREDIT BUREAUS

Credit has been used for many centuries. King Solomon used credit to build his temple and credit played an important part in the life and commerce of early Rome. Historical records show that the granting of credit was accompanied by considerable problems, and there were harsh punishments for debtors who could not repay.

Initially, credit was arranged between friends. The credit granter based his decision on his personal knowledge of the credit seeker and the proposed transaction. The important point is that the parties knew each other and their business histories well.

As population and trade increased, it became difficult, then impossible, to extend credit on the basis of personal knowledge. Credit granters simply couldn't be expected to know each individual.

As a result, credit was extended to applicants who were not acquaintances but who could show that they owned property. Next, credit was extended to applicants who were not property owners but whose credit could be guaranteed by property owners.

Demand for credit continued to expand, and credit granters found they didn't have the staff or the time to gather sufficient information on which to evaluate applications. They needed an independent, reliable and objective third party to collect this information. The result was the Credit Bureau.

The Associated Credit Bureaus of Canada

Credit Bureaus have been serving Canadians since 1922. The first Canadian Bureaus were formed by groups of merchants. They provided credit information by co-operative means, establishing offices to which members reported their credit accounts as well as applications for credit. In some communities, individual businessmen established privately-owned bureaus. Today both types exist.

As the number of bureaus grew and as the mobility of the public they served increased, Credit Bureaus introduced a system of inter-city reporting. Subsequently provincial associations were established and, in 1939, the Associated Credit Bureaus of Canada was incorporated under Dominion Charter as a non-profit organization.

Today the Associated Credit Bureaus of Canada has 153 member bureaus in all 10 provinces, employing approximately 2,500 persons. The national office of the association is located in Toronto. All member bureaus are bonded and licensed in accordance with the laws of the province in which they operate. Most Canadian Bureaus are also affiliated with the 2,000-member Associated Credit Bureaus Inc., our international trade association headquartered in Houston, Texas.

II THE MODERN ROLE OF CREDIT BUREAUS

Canadians enjoy a better standard of living than ever before because we are a credit-oriented society.

Credit has enabled Canadians to purchase immediately many of the things they might otherwise never be able to own. Items once considered as only hoped-for luxuries are now within the reach of virtually everyone.

The increased purchasing power available to individuals and business firms through credit is, in large measure, responsible for spurring the Canadian economy to its present record level. Continued growth of consumer demand, primed in great part by these credit facilities, has enabled Canadian industry to adopt mass production methods and thereby introduce economies of scale that benefit the entire nation.

To put it another way, if everyone had to save the full purchase price of a car, television set or refrigerator, there no doubt would be a substantial and severe reduction in the sales of these products which would reverberate throughout the economy.

The Credit Explosion

Today, our Society is experiencing momentous change as new ideas and technologies are developed. Consumer credit is no exception to this trend. New forms of consumer credit and increased services in existing forms have revolutionized the marketplace.

The "Credit Explosion" has featured a sharp growth in instalment loans, credit cards for almost every need, revolving charge accounts, and longer-term arrangements for purchase of goods such as automobiles and major appliances.

Outstanding consumer credit has multiplied five (5) times since 1951 to an approximate total of $9 billion today.

The Role of Credit Bureaus

Credit Bureaus play an important role in the credit process. ACB of C's 153 members provide more than 5 million factual and usually brief credit summaries a year, most of them by telephone, to more than 40,000 subscribers.

Members, 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;
- do not provide credit reports to everyone who seeks them.

A Credit Bureau is a clearing house for factual information, information supplied, in most part, by the accounts receivable departments of clients. This information is available only to subscribers and is on a confidential basis.

Under ACB of C policy, service contracts are required which certify 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.

To safeguard against unwarranted disclosure, Credit Bureaus refuse service to any prospective subscriber who will not enter into such a contract. Service is discontinued to any subscriber who fails to honor these provisions.

Membership Requirements

To become a member of the Associated Credit Bureaus of Canada, a bureau must first be a member of a provincial association. The provincial association will assist a new bureau in its infancy, but will not consider an application for membership until the prospective member has been in operation for at least six months, and is serving the majority of credit granters in his area. If the prospective member then shows evidence of financial stability, satisfactory references and ability to service the needs of the community, he is admitted on probation. Full membership is granted when the Board of Directors of the provincial association is satisfied that the Bureau will competently serve local and national clients.

Subscribers

Subscribers to our bureaus are credit granters. They in-

clude such businesses as automotive, finance, banks, department and variety stores, home furnishings, building contractors, oil and national credit card companies, real estate firms, and hotels and motels. They pay an annual fee plus a charge for each credit report requested.

To obtain this information, a subscriber must have a contract with the Bureau. He must identify himself by giving a special code number assigned on contract agreement. Only then is he able to obtain credit reports, which are generally transmitted by telephone. If he wishes a written report will be forwarded.

File information is never available to non-subscribers.

The Importance of Credit Bureaus

Of the 5,000,000 credit reports given to ACB of C subscribers in 1969, approximately 80 per cent were completely favourable.

Another 17 per cent were marginal. In this category are people who pay their bills, but with varying degrees of slowness. Only 3 per cent were unfavourable.

These figures indicate the valuable role Credit Bureaus play in Canada. Consumers with good credit records - and they are the great majority - can get credit quickly, easily and without embarrassment because Credit Bureaus provide quick, accurate summaries of credit background. A new-

comer to the community is extended credit as readily as a long-term resident who has established good credit habits.

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;
- delays in obtaining credit would result in the loss of sales and decline of business volume.

III BUREAU POLICIES AND STANDARDS

A major reason for establishing the Associated Credit Bureaus of Canada was to maintain high standards in the industry. We have developed a CODE OF ETHICS, and more recently a statement of CREDIT BUREAU POLICIES TO PROTECT THE RIGHT OF PRIVACY.

It is significant that the ACB of C voluntarily initiated the Policies. They constitute an effective system of self-regulation and precede any government legislation concerning the credit reporting industry in Canada.

Summaries of these two documents follow:

CODE OF ETHICS (APPENDIX I)

Sections relating to privacy are:

To assure information is factual and has not been altered, amended, coloured or qualified.

To adopt every safeguard for confidential handling of information by inquirers and employees of the Bureau.

To refuse service to anyone whose operations are illegal or inimical to the public good.

CREDIT BUREAU POLICIES TO PROTECT THE RIGHT TO PRIVACY (APPENDIX II)

The Right to Know

Bureaus will disclose to any consumer the information on file concerning that consumer, and will include in their

records statements of explanation given by consumers for failure to meet credit obligations.

Service Contracts

Subscribers must certify by contract that inquiries will be made only for the purposes of credit granting or other bona fide business transactions.

File Content

Files will contain factual material only. All input will be taken from the ledger experience of subscribers or the public record. No reference will be made to race, religion, political affiliation or personality. Specific content includes:

- Name
- Age
- Place of Residence
- Previous Places of Residence
- Marital Status
- Family
- Place of Employment
- Previous Places of Employment
- Estimated Income
- Paying Habits
- 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.

Time Limitations

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

Any adverse information which cannot be verified at source will be deleted immediately.

Personnel Reporting

Bureaus offering a personnel reporting service will ensure that specialized information will not be incorporated in credit reports or made available to subscribers inquiring about a consumer's credit record.

This statement on Privacy was intended to fully cover the six major areas of contention about Bureau operations.

"File" and "Investigating" Agencies

It is useful at this point to distinguish between the two major types of credit and personal information reporting agencies. The research study "Private and Commercial Reporting Agencies" (Legal Research Inst., U. of Manitoba, October/68) makes the following distinction:

"There are many different reporting agencies operating in most large cities, and no two agencies are exactly alike. It is possible, however, to classify them into two major types: those which basically act as information exchanges between groups of merchants operating in particular areas, and those which actively search for information on behalf of their members or customers. The former are often referred to as "file" agencies, and the latter as "investigating" agencies. The distinction is not an

absolute one, however -- companies which primarily carry on one kind of operation often at least dabble in the other."

The ACB of C members do not "dabble" in investigative reporting. Approximately 85 per cent of information comes from the ledgers of clients, the remaining 15 per cent from the public record. Members do not, for example, hire operatives to question neighbors or acquaintances.

ACB of C members handle the major portion of consumer credit reporting in this country. Members do not do insurance reporting, including life insurance or automobile insurance.

IV BUREAU PERFORMANCE IN PROTECTION OF PRIVACY

Accuracy

The University of Manitoba report states that "in spite of many precautions taken, a significant risk of error or misunderstanding remains". It recommends licensing as the method "to ensure that all members of the reporting profession continue to meet the exacting standards of accuracy which the leading agencies have already set for themselves".

We believe this statement suggests that accuracy is a potential problem, not a current one, and in fact, the industry is already policing itself adequately. (In this regard, licensing is superfluous.)

Notification

Various critics of the industry, or academics concerned with invasion of personal privacy, have advocated some form of notification to individuals whenever a Credit Bureau report is made on them. The ACB of C and its U.S. counterpart, Associated Credit Bureaus, Inc. have investigated this subject extensively, and strongly oppose it.

ACB of C research into this matter indicates that either proposal would drive the cost of credit reporting up by at least 50 per cent. This could cripple virtually every Credit Bureau in Canada as a viable business enterprise.

For example, according to individual Bureau estimates, either proposal would cost the Credit Bureau of Montreal $190,000 a year; the Credit Bureau of Greater Toronto $95,820 a year, and the Credit Bureau of Edmonton $72,750 a year. There would, of course, be additional hidden costs - such as those required for a greatly increased number of consumer interviews.

In the United States, where legislative activity on Invasion of Privacy is more advanced, Sen. William Proxmire, sponsor of the Fair Credit Reporting Act, was asked why some form of notification was excluded from the Act, which is the most advanced legislation of its kind. He replied: "I was strongly for that (notification). This was discussed by the Committee. It was discussed in the hearings at some length. We were finally convinced that this would involve so much expense, so much difficulty for the credit agencies that they had a legitimate complaint about it". (U.S. Senate Congressional Record November 6/69 513905)

A further factor in notification is the extent of consumer interest and/or dissatisfaction in relations with credit reporting agencies. Research (see next section) indicates that the general public has very few problems with credit reporting agencies and most of them are the result of believing that bureaus actually grant credit.

A.R. Walker, Registrar of the Ontario Consumer Protection Bureau, put it bluntly when he said in a recent speech that "it is the poor risk, who should not have credit anyway, who worries about what credit report is compiled on him...he is the crank that the small, vociferous segment of the public is listening to about privacy".

Access to Files

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.

If the consumer has been refused credit - and this is, of course, the most urgent reason for wanting to learn the contents of the file - the Bureau staff member conducting the interview will suggest the likely reasons for the refusal. He will offer suggestions and provide counsel as to how the consumer can take steps to rectify the situation.

Occasionally a consumer will question material contained in his file. The Bureau will check this data and will amend its files accordingly.

The extent to which consumers avail themselves of these services should indicate whether the general public

is concerned about privacy and accuracy of credit reports.

The conclusion, from research on customer complaints, is that the public has a low level of awareness of the bureau function and an almost infinitismal interest in the process of credit reporting.

The research program involved surveying all members of the ACB of C for the level of customer interviews and complaints in 1968. The results are given in Table I, reflecting the experience of over 80% of Canadian Bureaus.

It is obvious from these findings that:

a) There is some misunderstanding about credit bureau functions; and

b) The level of actual complaints about accuracy, invasion of privacy or any other problem is extremely small.

Credit as a Privilege, Not a Right

It is the contention of the ACB of C that credit is a privilege provided to customers by the credit granter, and not an inherent right. This distinction is important, because the public must expect to relinquish certain things - in this case, information on past credit performance - in return for credit granted.

TABLE I

Consumer Complaints Received and Interviews Completed

By Representative Sample of ACB of C 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.

Invasion of privacy, on this basis, has no application to the type of factual reporting done by members of the ACB of C.

We believe this distinction is made by the vast majority of individuals who show no reluctance in supplying the required information. They have realized there is little to fear and much to gain by full co-operation.

Summary

The ACB of C contends that member bureaus do not encroach on the individual's right to privacy. They supply factual history from information forwarded by other credit granters who have dealt with the individual concerned.

The arguments in support of this basic position are:

1. Credit reports are trade information. No reference is made to race, religion or political affiliation. No personal information is recorded based on comment of other individuals.
2. The consumer has access to his file. It is not kept secret from him.
3. The consumer can correct errors, question information or add extenuating circumstances to his record.
4. The information is confidential. It is only supplied to bona fide firms who require such in-

formation for the purposes of credit granting and for such business transactions as evaluating present and prospective credit risks.

5. Accuracy is a major concern. It protects both the credit granter and the applicant.

The development of additional regulations by government would, we believe, be redundant, costly and, if carried out to the extreme, would needlessly hurt both the industry and eventually the economy as a whole.

V THE EFFECT OF COMPUTERIZATION OF CREDIT BUREAUS

Basic Premise

We have previously stated the view that current Credit Bureau operations do not pose a threat to personal privacy. It is our contention further that computerization of Bureaus will not change this situation and in fact will promote greater accuracy and confidential treatment of file information.

U.S. Legislative Developments

Reference to a National Data Bank in the United States in the early 1960's has touched off an extended debate on potential invasion of privacy by data banks. Three major congressional hearings have been held:

1. The Gallagher Hearings, July, 1966 on "The Computer and Invasion of Privacy";
2. The Hart Hearings, December, 1968 on "The Credit Industry"; and
3. The Proxmire Hearings, May, 1969, on "The Fair Credit Reporting Act".

The major concern of U.S. legislators has been that there appears to be little control over the use of information stored in the computer. The most recent Proxmire Bill, which has passed the U.S. Senate, provides a federal law which clearly defines the proper usage of information in a credit bureau. Under the bill, it would make little or no difference whether the bureau was computerized or not. (In fact, the only area of concern as far as computers go was the difficulty of entering lengthy customer

statements in the file - this was solved by codes covering consumer statements.)

It is of key importance that the provisions of the Proxmire Bill on file usage, disclosure and updating coincide in all essentials with the Code of Ethics and the current ACB of C policies on protection of privacy. Current Canadian industry practices, in short, now coincide with this advanced U.S. legislation.

Specific Effects of Computerization of Credit Bureaus on Privacy

Three questions arise from the use of computers as they relate to privacy:

1. Do computers, by their very nature, permit far more extensive data bases to be built than might be possible on a manual basis?
2. Do computers introduce more room for error in a person's record, and do they make correction of such errors more difficult?
3. Are computers more conducive to fraud and misuse than are manual systems?

The position of the ACB of C on these questions is:

1. Do computers permit for more extensive data bases to be built?
   a) Computers are vehicles by which many credit bureaus' files can be consolidated into one metropolitan trading area. Such consolidation

holds many benefits to the credit granter and to the consumer. To the credit granter, it means he can now 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.

b) Computers are capable of handling larger data bases than possible manually. The real issues, however, are what types and amounts of information are held, and who controls it. Credit Bureaus serve as central depositories of factual credit-paying habits. They do not contain non-factual information or data on subjects other than those proven necessary to grant credit.

The real danger for consumers would be in having credit bureaus converted to additional purposes on a large scale, to become in effect a complete personal dossier. The ACB of C statement on privacy and purpose of business clearly prevents expansion of Bureau files to become complete personal files. (As an aside, it might be noted that the real

danger in this direction comes from government, with its knowledge of taxes, medical records, criminal and other court records, etc. The original outcry over invasion of privacy of course originated in the United States as a result of some theoretical references to a "National Data File".)

2. Do computers introduce more room for error and make corrections more difficult?

   a) Computers can control against errors more efficiently than is possible with manual systems, e.g.

      i. More checks for reasonableness of data input are contained in the computer systems than are possible on a manual basis,

      ii. Computers permit an automatic interface between the automatic billing systems of credit granters and the credit bureau's files.

   b) Computers for credit reporting are all on-line systems. Corrections of errors can be entered in these systems as quickly as they could be entered in any manual system.

   c) 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.

3. Are computers more conducive to fraud and misuse?

   a) Computers permit bureaus to have greater checks to guard against misuse of their files than was possible on the manual basis. In the (U.S. Associated Credit Bureaus computer package) Credipak System:

      . 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 granters' 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; and

      . the System produces lists of all significant changes made to files which require some supervisory review.

A 1969 IBM booklet, "The Considerations of Data Security in a Computer Environment", confirms that "the systems designer can help minimize potential (privacy) problems by programming significantly more comprehensive security checks than were possible with manual systems". For example, in order to eliminate accessing by unauthorized

employees on terminals, two actions are required - an "enabling" action by a supervisory terminal, and a specific sign-in procedure including personal identification by the operator.

We believe that the safeguards built into the Associated Credit Bureaus Credipak program are more than adequate to prevent abuses in the areas of privacy and accuracy.

Status of Computerization of Credit Bureaus in Canada

No Canadian bureaus are currently computerized or have firm plans to do so. Several segments of the industry, in major market areas, have conducted studies but for volume or other reasons have not proceeded as of this date.

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.

We believe also that computerization, when it comes, will take the form of a proven U.S. system, possibly the Credipak system of ACB Inc. It is very reasonable to expect that accuracy, privacy, updating and other problems will have been solved. This is certainly the case if Credipak, which can be purchased by Canadian Bureaus for a fee, is used.

On the basis of our studies to date, therefore, eventual computerization of the Canadian credit bureau industry should pose no more problems to personal privacy than computerization has so far caused in the United States. If fact, the time lag will allow Canadian bureaus to additionally profit by some years of U.S. experience in protecting the public and credit granters in this important area.

VI CONCLUSIONS

This Brief has attempted to establish that:

1. Credit Bureaus perform a highly important function in modern Canadian Society.
2. Canadian Bureaus, like those in the United States, have actively established a Code of Ethics and a position on privacy, and are living up to these policies. They deal only in factual information limited to that necessary for day-to-day credit decisions.
3. The most advanced legislation on credit bureau activities in North America, the Proxmire Bill, corresponds in its essentials with the procedures already being practised voluntarily by the Credit Bureau industry in Canada.
4. The general public is not very interested in the behind-the-scenes operations of Credit Bureaus, has few complaints and does not appear to regard credit files as an invasion of their privacy.
5. Computerization will not make any significant change in the industry's policies and performance on privacy.

ACB of C

Code of Ethics

To treat all inquiries uniformly whether they be from a local subscriber or an Associated Credit Bureaus of Canada member.

To abide strictly by the constitution, by-laws, rules, policies and ethics adopted by the Associated Credit Bureaus of Canada.

To build good member and public relations by fulfilling all responsibilities through honest, accurate and efficient credit reporting.

To refuse any and all requests to delete, alter, amend or qualify factual information in credit reports regardless of any coercion, threat or pressure.

To take every step necessary to ensure that information is factual and has not been altered, amended, colored, or qualified.

To adopt every safeguard for confidential handling of information by inquirers and employees of the bureau.

To refuse service to any inquirer whose operations are of an illegal nature or demonstrably inimical to the public good.

To work constantly for the proper use of consumer credit by both the public and the credit granter by fully supporting and cooperating with all business and educational organizations interested in consumer credit.

To provide a prompt and adequate service consistent with the principles of sound business operation relating to economy, continuity and the attracting of progressive management and personnel.

To strive continually for the elevation of the credit bureau industry among credit granters and the general public both locally and nationally.

Credit Bureau Policies to Protect the Right to Privacy

A. The Consumer's Right to Know

1. Credit Bureaus will disclose to any consumer the information on file concerning that consumer. This will be done on request, after the consumer furnishes proper identification.
2. Credit Bureaus will have personnel available during business hours to interview and counsel consumers seeking information about their credit records.
3. Credit Bureaus will not charge any consumer for an interview. Nor will Bureaus charge for any verification undertaken to amend items of record which have been questioned by consumers who have been denied credit. However, in the case of consumers who have not been denied credit, a nominal verification fee may be charged.
4. Credit Bureaus will include in their records statements of explanation given by consumers for failure to meet credit obligations as agreed. Such extenuating circumstances as prolonged illness and dissatisfaction with goods or services will thus be noted and reported to credit granters.

B. Service to Businesses and Professions

1. Service contracts will be required in which the subscriber certifies that inquiries will be made only for the purposes of credit granting or other bona fide business transactions, such as evaluation of present or prospective credit risks or evaluation of the qualifications of present or prospective employees.

2. To safeguard against unwarranted disclosure, Credit Bureaus will refuse service to any prospective subscriber who will not enter into such a contract, and will discontinue service to any subscriber who fails to honour the provisions of the contract.

C. File Content

1. Credit reporting files will contain factual information only. All input will be taken from the ledger experience of subscribers or the public record. There will continue to be no reference to the consumer's race, religion, political affiliation or personality.

2. Credit Bureaus will record the consumer's name, age, place of residence, previous places of residence, marital status, family, place of employment, previous places of employment, estimated income, paying habits and outstanding credit obligations. In addition, Bureaus may only record judgments and/or writs having to do with consumer debt; non-responsibility notices, registered chattel mortgages, conditional sales contracts and convictions under provincial statute and for criminal offences.

D. Time Limitations on Reports and Records

1. Credit Bureaus will report accounts placed for collection and accounts charged to Profit and Loss for not longer than seven years.

2. Credit Bureaus will report judgments for not longer than seven years.

3. Credit Bureaus will report bankruptcies of all types for not longer than 14 years from the date of assignment of the most recent bankruptcy.

4. Credit Bureaus will report records of convictions under provincial statute or for criminal offences for not longer than seven years from the date of conviction. After that period of time they will be stricken from the record.

5. Credit Bureaus will delete any item of adverse information when it is ascertained that the information can no longer be verified at source.

E. Personnel Reporting

Credit Bureaus offering a personnel reporting service will adopt rigid safeguards to ensure that this specialized information will not be incorporated in credit reports nor made available to subscribers inquiring about a consumer's credit record.

BIBLIOGRAPHY

Canadian Consumer Council
Report on Consumer Credit December/69

Privacy and the Law, Research Report No.1
"Privacy and Commercial Reporting Agencies"
Dale Gibson and John Sharp, University of Manitoba
October/68

IBM "The Considerations of Data Security in a Computer Environment" 1969

U.S. Senate Congressional Record November 1/69
S 13901-10 (Proxmire Bill)

"Invasion of Privacy by Consumer Credit Bureaus",
a report by the Advisory Branch, Research Council
of the Young Progressive Conservative Association
of Ontario February/70

"Report on Protection of Privacy in Ontario",
Ontario Law Reform Commission 1968, published by
the Department of the Attorney General of Ontario

"Personal Privacy in the Computer Age", Arthur R.
Miller, the Michigan Law Review, Vol.67, No.6,
April/69

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 3

Projections of the Impact of Technology on the Development of Large Data Base Information Systems

by

B.B. Goodfellow

IBM, Canada

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

PROJECTIONS OF THE IMPACT OF TECHNOLOGY ON THE DEVELOPMENT OF LARGE DATA BASE INFORMATION SYSTEMS

****

Conference
on
Computers: Privacy and Freedom of Information
Queen's University, Kingston, May 21-24, 1970

B.B. GOODFELLOW

ABSTRACT - Projections of the Impact of Technology on the Development of Large Data Base Information Systems

Computer technology has developed rapidly over the past 20 years and it is clear that we will continue to have significant developments in Central Processors, Storage Devices, Communications Systems and Programming Languages. These developments will help us build bigger, more efficient and more productive hardware. However, we are already beginning to experience architectural constraints on information systems development. These constraints will slow our progress in the development of data banks until more effective search algorithms and more efficient machine organizations are discovered. The security of information in such systems has become of concern. While there are potential problems in this area, development should continue since present and projected technology are more than adequate to protect us from unauthorized use of such systems.

B. B. Goodfellow

When digital computers were first introduced in the early 1950's, predictions for their use in industry ranged from the simple replacement of punched card installations to the all-powerful systems that would be an integral part of the management of large corporations. Concerns were also expressed about their impact on society. In spite of the many time-saving applications that were being installed and forecasts of new uses that would be essential to our economic growth, there were many who were convinced that the benefits derived from the computer would be outweighed by serious threats to our whole social structure. There were predictions of massive unemployment and concerns that the decision-making ability of computers would reduce management's role to a mundane level. Some predicted our most astute scientists would not be able to comprehend the rate at which this new tool could solve complex equations. In retrospect, those threats appear to have been groundless.

Today, however, we hear a new concern centering on the use of computers for the storage of data that will make up large information banks. The concern is invariably heralded as an invasion of privacy. The purpose of this paper is to discuss technology now in the laboratories as a basis for projecting how these developments will affect the evolution of computer systems. An examination of these systems will then serve as a guide to measuring the validity of the concerns about the operation of large information retrieval systems.

I would like to make it clear that my personal position is that while technological developments may represent a potential threat to privacy, this same technology may be even more important to us 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. The subject of this paper, however, will be to review technology today as it affects computer development and I will leave the predictions of their use to the other speakers on this program.

Analyzing forecasts in the computer field, we generally find short-term forecasts to be overly conservative and long-term forecasts to be somewhat optimistic. In trying to see why this has happened, I believe it is because predictions which assess the impact of technology are usually defined in an environment that is socially and economically static, while the specific technology under consideration grows at an accelerating rate.

In projecting the impact of technology on computers in the late 1970's, one must also project some aspects of the social structure that will exist at that time. The situation is not unlike the Heisenberg principle of uncertainty -- computer technology will be an integral part of a

society which is dramatically changed by that technology such that if we could accurately predict computer developments ten to fifteen years in the future, we would not recognize the environment they were in and the converse.

The same technology that will be available for the development of larger and faster computers will equally be applied to the development of different forms of information transmission which could lead, for example, to significantly different forms of government. It will also allow us to develop communications systems with audio and visual data, that could make the mail service as we know it today obsolete. The newspaper industry might similarly be obsolete and in fact it will be technically possible to have Government referendums on virtually every major issue.

Therefore, in looking at the place of computers or large data banks in our society, we must make a concerted effort to project the environment in which that data bank exists, for as I mentioned in my opening remarks, the computer data bank may not provide a threat but in fact the only promise of privacy in such a community.

In assessing the impact of technology on the development of large data banks, I believe it is appropriate to segment systems into

their essential elements analyzing the impact of technology on each area separately. The cumulative effect of these changes can generally be inferred in the context of the particular application. The major elements of system development to be considered are:

1. The Central Processor including systems organization;
2. Storage media
3. Programming
4. New Application areas

I would now like to comment briefly on what we can expect in each of these areas.

CENTRAL PROCESSING UNIT

At this time it is fairly safe to predict that silicon monolithic semiconductor technology will dominate central processor design for the next ten to fifteen years. Since the early 1950's, the cost/performance of electronic components has improved by 30 to 40 per cent per year, while overall system performance, including input/output and external storage media has improved by about 20 to 25 per cent per annum. There is little reason to believe these trends will not continue; however, the very high research costs for the

development of integrated circuit technology and more particularly the high cost of manufacturing processes for this technology will have significant impact on projected trends particularly in the cost element of the price/performance equation.

In the medium to low cost systems, thick and thin film circuits are generally available in the 100 to 500 nanosecond range. Intermediate systems using monolithic systems technology in the 5 to 10 nanosecond ranges are also available in limited numbers today. 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. The reasons for projecting this limit centre around the problems of cost, heat dissipation and the physical connection of logic elements to other parts of the system. It is interesting to note that in the past two or three years, increased functional density has been achieved primarily through circuit innovation rather than the shrinking of geometrics and design tolerances or the introduction of new processes such as multi-layer interconnections.

In any case, today we can visualize the technologies that will take us to absolute limits in CPU performance. Based on the very

limited experience with the design of current information systems, it is projected that search times will have to increase between a thousand and five thousand times to make even relatively simple information systems practical. The projections of circuit improvement do not support such increases and we will, therefore, have to devise either new search algorithms or develop new methods for computer organization. Improved search algorithms are elusive and there is little evidence of improvements in this area available today.

In computer organization, the current indication would be the development of multiple processor systems operating under the control of a master operating system. A number of breakthroughs will also have to occur in this area before system performance will satisfy the implied requirements of many of these proposed data banks. One of the approaches which will undoubtedly be considered in the design of improved performance CPUs, will be the use of hierarchical memory structure similar to that now employed in the IBM /360 Models 85 and 195.

Briefly, limited banks of integrated circuit technology will be used to provide not only logic functions but also storage capability at the operating limit of the technology. For cost reasons, it will not be practical to have the entire CPU storage use this concept and large banks of core or thin film storage will act as back-up storage devices.

For the most part, these will be transparent to the programmer and system degradation will be only slightly below that of the CPU capability.

In summary then, CPU performance in the picosecond range is clearly practical with known technology. It would also appear to present some absolute limits of circuit performance and since this may still be well below that required for many applications, new system organizations will have to be considered.

Considering the development of CPU and bulk storage, it appears that core technology is rapidly being exhausted and is generally reaching the point of diminishing returns. Although further development effort will still be applied to bring about improvements, these improvements will be less and less significant to performance. As mentioned previously, integrated circuits have potential as a replacement for core; however, cost considerations suggest that we are quite a piece away from seeing core completely displaced.

Need, however, is also a consideration and faster switching times will dictate the use of media other than core. State-of-the-art switching for cores is generally in the 200 nanosecond range. Considering the additional memory cycle required, the cycle time for large core memories is likely to remain in the 500 to 600 nanosecond region for the next few years.

Thin films offer one avenue which appears to have the potential for switching in the 100 nanosecond time frame. Although films are potentially much faster, they are still plagued with the same problems core memories encounter -- those of decoding a large drive-line array; and the amplification of currents of a few hundred milli-amperes in the inductance of the magnetic array and interconnect wiring. These processes take time, time that is inversely proportional to the cost of reducing it. The cost of producing memories is a difficult comparison to make but if we assume core with a unit cost of "one" per bit, these costs have generally remained constant since 1967. Films have a projected cost at about two-thirds this value which will be attainable in the 1971/72 time frame. Integrated circuits, however, and particularly large-scale integration offers potential cost reductions significantly below this figure by the mid-1970's, and it is safe to project that integrated circuitry will represent the bulk of CPU static memories by the end of the 1970's. These memories will be close to the limit of electrical technology but will not be fast enough for many large data bank applications without significant improvement in search algorithms or unique approaches to system organization.

STORAGE

The development of improved bulk or dynamic storage media will also continue but as we have already seen, at a less dramatic pace than occurred in the early 1960's.

Magnetic tape densities will undoubtedly increase but it is fairly clear that the use of tapes in large information systems will be primarily for historic record. Random access devices will have increased density and increased capacity. It is an unfortunate fact that increasing storage generally increases access time and in projecting ultimate levels of performance in speed/capacity/access one can obtain a good estimate of the trend by analyzing the various forms of existing storage such as punched cards, magnetic drum, magnetic core, magnetic tape or disk files. A figure of merit can be developed by expressing the bits per cubic measure of storage as a function of its per second access time. (This latter figure not to be confused with the transfer rates of the system).

Analyzed this way, it is clear that new storage devices can provide the required capacity for most information system applications but as noted previously, improved search algorithms will have to be found to make them practical for many of the systems considered. Projecting the analysis of our progress in developing storage media,

including both capacity and access time, to the genetic level where our storage system is very compact and subtle but often imprecise, we see plenty of room for improvement in the current state-of-the-art.

Magnetics, of course predominate and are popular because they achieve high densities and can be erased any number of times and yet are permanent when desired. A number of alternatives will also be considered in the future -- thermal plastic, photo plastic, electrostatic, cryogenic, ultrasonic, optical and dielectric technologies. In addition, radically different approaches such as electron spin echo must be examined even where probability of application is slight. Perhaps the chemical or molecular biological memories of living beings will be imitated, but this seems to be in the very remote future. It is interesting to conjecture whether we can make effective use of such memories by association, or by learning processes, or forgetting less useful information, or of gradually moving information to less accessible places to clear the way for current data. Clearly breakthroughs such as this must occur for these devices to be practical for the very large storage application. Dates by which such innovations will occur cannot be forecast with any degree of certainty.

In summary, Random Access storage based on magnetic recording has considerable potential for improved performance in large data base applications. 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 will have unacceptable access times to operate in real-time mode. Some of the new technologies may overcome the basic limitations encountered today but these systems appear to be beyond a ten-year forecast.

PROGRAMMING

Programming Systems have generally developed in response to need and, in the case of information systems, the need is still unclear primarily for reasons related to the lack of better search algorithms. There is an obvious need for improved languages which will respond to transactions entered from interactive terminal devices. The system will be transaction driven and programming systems must be developed to provide better response to this environment.

Secondly, we can anticipate changes in the basic structure of a "program". This structure has not really changed much (other than in terms of richness of language) from the early machine language codes. These early programs and most programs today contain statements which define access methods, files, records and fields as well as statements which define logical procedures to be performed on those fields. With the advent of System/360 operating systems, some of the physical file handling statements were consolidated into operating system routines. In the future, we can anticipate that

almost all statements dealing with data definition and input/output, will be consolidated and separated from the problem or procedural segment of the program. The program will concern itself only with the logical operations to be performed on the data and will simply request data by file name. The elimination of embedded data definition from the program is an important architectural requirement of many information systems.

Focussing on the language itself, we will undoubtedly see increasing use made of what can best be described as problem-oriented languages. Concepts used in the IBM System/360 Model 25 suggest how these might develop. Using a microcode structure for the completion of logic functions, one can envisage the development of hardware which has essentially no personality of its own. Every customer, or as a minimum each industry, would have its own specific requirements in terms of instruction set, data format, etc., and special programs loaded into the microcode of the system would give the machine its personality. Operating systems to respond to the terminal requirements I mentioned previously would reside in this environment and application programs would actually be a third or fourth level program in the system.

Such programs have the potential for considerable inventiveness in terms of security which have not been studied in depth at this time. A wide variety of procedures for the coding, mixing and otherwise cryptographic fusion of information exists and to the best of my knowledge, the ease with which these procedures could be implemented far exceeds the deciphering techniques that might be devised for them. Clearly, any coded system can be deciphered, but there is a very real question of its value vis-a-vis the use of the data and I would refer you to a booklet available from IBM on "The Considerations of Data Security in a Computer Environment" which outlines some of the approaches which can be considered for protecting the security of data files.

In summary, new problem- and industry-oriented languages will develop in response to need and improved hardware design. These programs plus the use of some simple coding systems which can easily be implemented today provide adequate protection for most applications. The cost of developing more complex protection for high security data is probably well below the value of the data to persons attempting to obtain it illegally.

NEW APPLICATIONS

Let's for a moment consider the implications of what I would define as the invalid conclusion that we cannot adequately safeguard computer based information systems. Would that justify the passing of legislation to prevent their development? The answer is clearly no. While some systems such as those including data on our line of credit, health or criminal records should not be established without satisfactory protection, there are a host of other applications which do not impinge on personal privacy which must be developed if we are to take full advantage of the technology that is available to us.

With big enough and detailed enough repositories of information on people, for example, doctors could spot the first appearance of a new disease in a community and cure it before it reached an epidemic. Educators could identify throughout our society, brilliant children barred for some reason from the chance at a college education and try to help that child's family remove the obstacle -- an obstacle which deprives us all. Recognizing the value of such information, the arguments for centralizing it by electronic means are compelling. Specifically to the policeman who has flagged down a speeder, it means knowing - as he approaches the stopped car - whether he is about to confront a happy-go-lucky teenager or a trigger-happy

escaped convict. That knowledge can save his life.

In a time when cities and people move about as never before, electronic centralization of data helps local governments know what is going on -- helps them see problems coming, before they boil over into traffic snarls, over-crowded school buildings and inadequate employment opportunities. We cannot become intellectual Luddites and ban technology for that would be to admit we cannot control our own creations. It presents a challenge, but one that I believe we clearly can manage, and in fact must manage if we are to take full advantage of the many benefits technology offers for our very survival.

In closing, I would like to recall an episode in the life of Sir Winston Churchill - when he was a young man in India during the late 1890's. He later recalled an incident when he and his comrades one gay evening joined in a rousing song of alarm over the X-ray camera -- a shocking invention in his words "enabling photographs to be taken through a screen or other opaque obstruction." With the arrival of this awful new wonder, Churchill observed tongue in cheek "it appeared that there might soon be an end to all privacy."

References and Further Reading

1. Computer Privacy - Hearings before the Subcommittee on Administrative Practice and Procedure - United States Senate - March 14 and 15, 1967

2. E. D. P. Analyzer - January 1970 Volume 8 No. 1
Progress in Information Retrieval

3. Trends and Implications of Current Legislation Dealing with Computers and Invasion of Privacy
Professor A. R. Miller - University of Michigan Law School

4. The Third Listener - John M. Carroll
Publisher E. P. Dutton

5. Architectural Questions of the Seventies
L. D. Amdahl - Datamation, January 1970

6. Information Storage Density - Marvin Camras
IEEE Spectrum, July 1965

7. The Considerations of Data Security in a Computer Environment - IBM Publication

8. Technology and Privacy - Address by T. J. Watson, Jr. to the Commonwealth Club of California, April 5, 1968

9. Large-Scale Integration - A status Report
D. E. Farina - Datamation February 1968

10. What's Next in Memories - D. Mayne
Datamation February 1968

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

BACKGROUND PAPER NO. 5

Report on Protection of Privacy

Ontario Law Reform Commission 1968

Department of the Attorney General

*****

DOCUMENT NO 5

La protection de la vie privée

Un rapport de la Ontario Law Reform Commission, 1968

Ministère du Solliciteur général

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

In its last Annual Report the Commission identified the Right to Privacy as an important area of interest. Accordingly, in May 1968, the Commission arranged with Professor Edward F. Ryan, of the Faculty of Law, University of Western Ontario, to conduct a preliminary study of the problem of protection of privacy in this province. That study has now been completed and is attached as an appendix to this Report. Although Professor Ryan's study stands by itself, the Commission wishes to add that every part of the applied scholarship that it contains can be supplemented by evidence of practices that both shock the conscience and intensify the increasing apprehension that is felt in this province and in Canada for the need for protection of the privacy of the individual.

Professor Ryan's study is the first detailed study of this problem produced in Canada. It examines first the broad aspects of the problem and then deals with three important areas:

1. constitutional considerations;
2. the existing federal and provincial law; and
3. measures that should be considered in Ontario.

This study shows that a province has, both analytically and practically speaking, a considerable amount of room in which to legislate in relation to privacy. One of the major themes of the study is that privacy is a new field in legal and constitutional thought.

The portions of the study dealing with existing legislation take a critical look at those federal and provincial statutes that protect, threaten or affect privacy in some way or another. This review of statutes demonstrates

that individual privacy has very seldom been viewed as a separate aspect of legislation, that is something to be protected for its own sake, or as something that must be considered in legislation dealing with other matters of public, social or economic interest. Privacy has not been taken into account in most cases.

The heart of the study is the twenty-point proposal for measures that should be considered in Ontario, contained in Part Five. In a few words Professor Ryan has summed up the objectives that must be pursued if we are to re-establish the place of privacy in our modern world. These recommendations speak for themselves.

PART FIVE: MEASURES THAT SHOULD BE CONSIDERED IN ONTARIO

I. A twenty-point proposal

It is hoped that at this point in this report, the reader will have a good overall view of the major considerations that define the problem of protection of privacy. The constitutional difficulties that arise are intricate but not insurmountable, and a major provincial legislative programme for the protection of privacy could be undertaken without either the danger of straying into an occupied field, or leaving the penumbra of section 92.[168] The selection of Ontario legislation illustrates that this province is behind some of the others in Canada in moving to deal with modern privacy problems, and the selection of legislation from other jurisdictions indicates that no one has yet attempted in Canada to muster the necessary implements of protection that modern conditions demand. The approach to the protection of privacy in this country has been episodic and fragmentary, poorly conceived and only incompletely executed.

One of the major flaws in the collective Canadian approach evidenced by the mixed bag of statutory provisions set out above is that legislatures have been primarily concerned with treating the symptoms rather than trying to cure the disease. The preoccupation with wiretapping is one significant manifestation of this. 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 (and the writer thinks that this is a proper starting point), 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.

With these considerations in mind, the writer recommends that a full investigation into the protection of privacy should give serious and thoughtful attention to the following categories and subjects of concern:

1. Creation of the offence of invasion of privacy.

2. Creation of the tort of invasion of privacy, with appropriate remedies.

3. Establishing controls over the sale, advertising, use and possession of mechanical and electronic wiretapping, eavesdropping and surveillance devices.

4. Establishing controls over governmental acquisition, use and disclosure of personal information, with appropriate personal remedies.

5. Establishing controls over private sector acquisition, use and disclosure of personal information, with appropriate personal remedies.

6. Creating rules for electronic surveillance, wiretapping and surreptitious invasion of privacy in all forms to control abuses in the administration of justice in the province.

7. Creating rules to control the use of security devices as a means of secret surveillance.

8. Defining "consent" in its various contexts where consent means that privacy is not invaded.

9. Defining the extent to which an owner of public accommodation facilities owes a duty to patrons to not participate in activities which violate their privacy.

10. The encouragement of the development of organizational and professional ethical standards for the protection of privacy.

11. Establishing controls over certain conditions of employment which violate the right to privacy.

12. Developing mechanical and electronic safeguards to control unauthorized output of personal information from computer memory banks.

13. Specific legislative regulation of the conduct of persons and institutions, the legitimate activities of which per se establish a threat to privacy.

14. Making contracts that have as their object the unwarranted invasion of privacy of a third party void ab initio.

15. Giving consideration to the inclusion of privacy as a fundamental right in the proposed Ontario Bill of Rights.

16. Establishing rules that create the highest degree of visibility for all surveillance by the "public authorities" that can be attained without unduly hampering the achievement of valid social ends.

17. Encouraging the establishment of a parallel federal investigation with complete provincial-federal cooperation to ensure the creation of complementary controls that are effective measures for the protection of privacy.

18. Reviewing and recommending appropriate changes in all provincial legislation in which the considerations of privacy have not been afforded adequate protection.

19. Establishing and promulgating a definitive public policy against any routine compilation of a "life history" dossier or profile either by government or by the private sector or by any combination thereof.

20. Creation of an independent agency with educational, persuasive, evaluative, investigatory, decisional, regulatory, reporting and coercive powers to protect and foster the right to privacy in all of its aspects.

These twenty points all involve normative judgments in the light of a multitude of legal and social facts. Some of these latter data are

matters of general knowledge, some can be safely assumed, and others call for specific research. In the following pages, this report will deal with some of the significant points raised above without necessarily making a fine distinction between values and assumptions and facts. These are simply subjective observations which both point out alternatives and suggest solutions to the problems inherent in these twenty points.

168 It should be emphasized that the constitutional problems in the privacy area have been dealt with only in the abstract. Definitive answers thereto must be sought when we draft definitive legislation. However, most of the broad principles that seem to the writer to bear on the subject matter of this report indicate that the province may legislate with considerable freedom.

169 Cf., The Prohibition Act, Stat. P.E.I., c.27 (1937), as amended Stat. P.E.I., c.9 (1943) s.88: "No property right of any kind shall exist in liquors unlawfully kept at any place in this Province."

170 See generally MacDonald, The Licensing Powers of the Province, 17 Can. B. Rev. 240 (1939).

171 Subject to the possible limitation that the legislature of one province cannot destroy civil rights outside the province by interference with contractual rights. See Ottawa Valley Power Co. v. H.E.P.C. [1937] O.R. 265, 304; Beauharnoir Light, Heat and Power Co. v. H.E.P.C., [1937] O.R. 796 (Ont. C.A.).

CONFERENCE

ON

COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION

QUEEN'S UNIVERSITY

MAY 21-24

1970

POSITION PAPER

PANEL 5

File Security for a Shared File, Remote Terminal, System

by

David F. Booth

I. P. Sharp Associates

CONFÉRENCE

SUR

L'ORDINATEUR, LA VIE PRIVÉE ET LA LIBERTÉ D'INFORMATION

UNIVERSITÉ QUEEN'S

21-24 MAI

1970

FILE SECURITY FOR A SHARED FILE, REMOTE TERMINAL, SYSTEM

By David F. Booth

I.P. Sharp Associates

RESUME

File Security for a Shared File, Remote Terminal, System

by David F. Booth

This paper describes a very recent and advanced implementation of a file handling system which enables a number of remote system users to have controlled access to the same or different files while retaining a high degree of file integrity and security. The system is known as the APL Shared File System.

File integrity is part of the APL Shared File System design. In brief, file security is achieved by writing short access functions which contain file handling commands and/or user screening tests and/or data selection operations. The access functions are locked to prevent security codes or partially processed data from being disclosed. Access codes associated with file handling commands make the locked access functions useless to all but the authorized user. The authorized user gains access to the system via an account number and a password which can be changed at any time. Further details and examples are found in the main text of the paper.

RÉSUMÉ

Sécurité des dossiers dans un système de dossiers partagés à terminal éloigné

par David F. Booth

Cette communication décrit une application très récente et très moderne d'un système de manipulation des dossiers qui permet à un certain nombre d'utilisateurs éloignés d'avoir un accès contrôlé aux mêmes dossiers ou à différents dossiers tout en gardant un haut degré d'intégrité et de sécurité des dossiers. Ce système est connu sous le nom de Système de dossiers partagés APL.

L'intégrité des dossiers fait partie de la conception du système de dossiers partagés APL. En résumé, on assure la sécurité des dossiers en rédigeant de courts programmes d'accès qui contiennent des commandes de manipulation des dossiers et(ou) des tests de criblage des utilisateurs et(ou) des opérations de sélection de données. Les programmes d'accès sont verrouillés afin d'empêcher que soient révélés les codes de sécurité ou les données partiellement traitées. Les codes d'accès associés aux commandes de manipulation des dossiers rendent les programmes d'accès verrouillés inutiles pour tous les utilisateurs, sauf pour l'utilisateur autorisé. Celui-ci a accès au système au moyen d'un numéro de compte et d'un mot de passe qui peuvent être modifiés à n'importe quel moment. De plus amples détails et des exemples sont donnés dans le texte de la communication.

Introduction

This paper describes a very recent and advanced implementation of a file handling system which enables a number of remote system users to have controlled access to the same or different files while retaining a high degree of file integrity and security. The system is known as the APL Shared File System.

APL is A Programming Language which permits efficient interactive computer processing via remote terminals. The Shared File System augments this capability in the area of file handling.

File Processing Needs

From the time that the technical problems of time sharing and computer communications were mastered, the number of applications for remote terminal systems has soared. It is not too difficult to see why these systems are so attractive. In the first place, the programmer and the non programming user need not leave the environs of their work place. Secondly with computer languages like APL an interactive mode of operation is introduced which enables the computer to guide non-technical staff to error free communication with the machine. Thirdly the system can be interrogated or updated at any time by as many people as its design permits, so that information is up-to-date no matter where the user is located.

It is not surprising that airline reservations systems are being built and that banks are already designing remote terminal systems to handle public accounts at the teller's wickets. Inventory systems, credit control and management information systems take on new meaning with the advent of remote time-shared systems. However, it is also apparent that by placing the computer access outside the computer room with no human monitoring of a multitude of users, considerable responsibility for data security must be left with the system. Added to this, there are a considerable number of people who would like to take advantage of remote terminal time-shared systems who can not afford to have their own dedicated facility. Put two or more of these people on the same system and there is not even a sense of corporate unity to deter the 'file-cracker'.

It would be difficult to improve on the concise, thorough survey of the weak points and security precautions of remote time-shared systems that is contained in the IBM publication 520-2169-0* 'The Considerations of Data Security in a Computer Environment'. However, for completeness, it is worth noting the prime areas of concern and action.

---

*To be distributed at the conference on 'Computers: Privacy and Freedom of Information' Kingston, Ont. May 21,70.

(a) The user must show he has authorization, in such a way that it is difficult for him to be impersonated.

(b) It should be possible to control the degree of access of each user to any data.

(c) Testing security programs is a vulnerable period.

(d) The communication link can be intercepted both passively (which is difficult to detect) and actively.

(e) Data must not be accessible to computer operations staff, though they are probably expected to handle and safeguard the physical storage media.

(f) Physical locks, identification cards and the older forms of data protection still have their place.

(g) Illegal attempts to obtain data should be recorded as they happen and the appropriate authority noted.

(h) Legal accesses could be recorded.

(i) Personnel should be selected carefully.

Let us look at an actual solution to the problem which shows that a considerable degree of security can be obtained economically through software techniques. What is more the degree of security employed is in the hands of each file designer, which is important because security usually costs money in both users time and computer costs.

Some Relevant Features of the APL Language and System

Many of the attributes of the Shared File System are derived from the parent language APL, so that it is worth introducing one or two crucial features on which file security depends.

Each APL user is given at least one sign on (account) number, typically of 7 digits chosen at random. While this code may remain unchanged for many months the user may append his own password of up to eight characters and change it at any time. To gain access to the system the account number and password are typed at the terminal and checked by the computer for authenticity. It is often desirable to obscure the typed characters. One possibility is to depress the tab key as the code is entered so that each character overstrikes the previous input.

When signed on the user has several options open to him. He may process data on a once off basis as it is entered by means of a number of primitive operators on the keyboard e.g. add, take logarithms, sort, compare words etc. Alternatively he may decide to write a program composed of the primitive operators which will later be called as though it were a primitive operator itself. Or he may ask for the execution of a set of previously defined programs on some specified data. In general, there is very little difference in these modes of operation.

The most important point to note is that when an APL function is written it can be locked so that no one, not even the function designer or the APL console operator, can see how the program works, or can change it. It can never be unlocked. It can only be erased. Unlike some computer languages, APL primitive operators cannot read or modify other primitive operators, so that the locked APL function is entirely secure. For this reason locked APL functions are an important tool in file access control.

Not only can the user protect his account number and the contents of his programs but also units of storage called workspaces. 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.

A Summary of Shared File System Controls

To the user, the Shared File System is a consise set of one word commands with qualifiers. From these commands a *FILE* can be created with an assigned name. It can then be built up to any size within reason, *COMPONENT* by component, with each component being any allowed APL expression or array of data. Any component can be read, deleted or modified.

For the sake of 'bookkeeping', it is possible to find out how many components are assigned to each file, the storage space occupied by the file, the names of files accessible to the user and those which he is currently using.

The owner of a shared file may review and modify a list of authorized file users and their degree of access. The shared file user can temporarily preclude access by others to a set of specified files.

Fundamentally the primitive commands are of the form:

FREAD 36 12

: i.e. Read File 36, component 12. The contents of the 12th component is then immediately available for further processing: e.g. if the contents of the 12th component is a string of numbers they may be summed using the APL summation symbol +/.

+/*FREAD* 36 12

The majority of primitive commands may be assigned an access code number by the file designer, which links a specific user sign on number to the contents of that file: e.g. in, *FREAD* 36 12 29175, the 29175 is the access code. To be able to read file 36 the user must sign on with his own account number and the current password and must use the *FREAD* statement with the correct access code. However, rather than impose the burden of remembering several access codes, the intention is that the *FREAD* statement and code, be incorporated in a locked APL function: e.g.

```
        ∇ SECUREREAD N
[1]     +/FREAD 36 N 29175
        ∇
```

So by typing, *SECUREREAD* 3, the sum of the elements of the third component of the file 36 is produced and printed for the authorized user. The locked function can contain numerous types of data screening or access restrictions written in APL e.g. from a file component containing both telephone number and salary only the telephone number might be selected, or there may be a time of day test which restricts the time that the night watchman accesses the file.

In general the user will have a number of locked access functions stored in a workspace which permit various degrees of access to a number of files. To gain

access he evokes the appropriate function and in fact never sees the access code. There is nothing to prevent the file designer from assigning a locked function with one or more access numbers to several users, who are to have the same degree of access.

The system maintains a table of access codes, authorization, and user numbers for each secure file. With the appropriate access code this table itself may be inspected and modified, so that the responsible party may cancel any authorization at a moment's notice.

Should an unauthorized user obtain a copy of a locked access function it is of no use to him since the access code and his account number are not shown together in the table of access codes. His illegal attempt to use the function is logged by the system and the appropriate authority can be notified should illegal attempts exceed a threshold. The legitimate user may change his sign on password whenever he chooses which makes it extremely difficult for the unauthorized user to sign on with the legitimate users number. Should the file designer be hyper sensitive about security there is no limit to the number of dynamic tests which can be incorporated in the locked APL function. Presumably these will be chosen so that the legitimate user will remember the correct response!

The Shared File System Applied

Perhaps the best way to describe the security facets of the shared file system is by the use of an example, somewhat simplified for clarity.

Assume that as part of a Management Information System there is a combination of personnel record and personnel work load data. For each employee number there are entries such as age, sex, salary, experience,education, department, scheduled work load, and commitments, start date, finish date etc. Various employees are to be permitted access to this file. For example, the Director of Personnel may see all entries. His assistant may add new names with their associated personnel records, he may update the personnel aspects of old records. He may delete information on ex-employees two years after they have left.

Certain members of the Accounting Department are to have access to names and salaries and as a precaution their authorization must be renewed by the Chief Accountant on the first day of each month.

Project, Section and Department Managers are to have access to all details of staff under their direction.

Information System Structure

Although the data may well be processed serially to produce the payroll output, a considerable number of the accesses will be random by employee number. For the sake of efficiency a directory of employee num-

bers with pointers to the employee data is maintained. For example this might be a file called *DIRECTORY* designed for five digit employee numbers, with the first two digits synonymous with a component number of the file. Within each file component is a table of 3 digit employee numbers with associated integer pointers to the main file entries. Note that only the personnel department is allowed to update the directory, all other employees may read it. In practice directory updating is taken care of by a *NEWEMPLOYEE* program, and an *UPDATE* program.

Three further files are created called *ALPHA*, *NUMERIC* and *SCHEDULE*. Processing is simpler if alpha data is segregated from numeric data and is more efficient if segments with different usages are separated.

Fig. 1

The Nth component of each file contains information appertaining to one employee. So by requesting:

(FREAD 3 N) [5]

: file 3, component N is read and the 5th number is extracted i.e. Start Date.

It may be that data on a new employee is to be entered in which case:

'EMPLOYEE NUMBER'

'NAME SEX DEGREE TITLE EXPERIENCE' FAPPEND 2

'DEPT SALARY AGE EDUCATION SDATE FDATE' FAPPEND 3

BLANK ENTRY FAPPEND 4

: is all that has to be entered to update the record.

DATA BANK STRUCTURE *FIG.1*

FILE 2 *ALPHA*

COMPONENT

1 *NAME SEX DEGREE(S) TITLE EXPERIENCE*

2

3

-

-

N

-

FILE 3 *NUMERIC*

COMPONENT

1 *DEPT SALARY AGE EDUCATION START DATE FINISH DATE*

2

3

-

-

N

-

FILE 4 *SCHEDULE*

COMPONENT

TIME ALLOCATED, WORK COMPLETE, WORK LEFT, UPDATED

1 *JOB 1* --- -- -- ------

JOB 2 --- -- -- ------

JOB 3 --- -- -- ------

ETC

2

N

-

Full advantage should be taken of the systems interactive capabilities by writing a short program which asks for each input by name and if necessary spells out the form of the reply, so avoiding sequence or format errors. e.g.

The user types	*NEWEMPLOYEE* (or some abbreviation)
The system responds	*NUMBER?*
User	29315
System	*NAME?*
User	*RYCO J.*
System	*SEX (M OR F)?*
User	*M*
Etc.	
System	*START DATE (DAY MONTH YR ------)?*
User	020570
System	*MORE (Y OR N)?*
User	*N*

At completion the directory and files 2, 3 and 4 will be up-to-date.

The assistant to the Director of Personnel would be given three locked access programs e.g.

NEWEMPLOYEE, *UPDATE*, *EXEMPLOYEE*

The program *NEWEMPLOYEE* might look something like:

```
     ∇ NEWEMPLOYEE
[1]    DIRECTORY FTIE 1 529147
[2]    ALPHA FTIE 2 529147
[3]    NUMERIC FTIE 3 529147
[4]    SCHEDULE FTIE 4 529147
[5]    'EMPLOYEE NUMBER?'
[6]    (F,L)←SPLIT EN←⍞
[7]    →(L SEARCH FREAD 1 F 529147)/CONTINUE
[8]    →0,⍴⍞←'NUMBER ALREADY ASSIGNED'
[9]   CONTINUE:'NAME?'
[10]   INPUT2←⍞
[11]   'SEX (M OR F)?'
[12]   INPUT 2←INPUT2,⍞
[13]   ETC(COLLECTS DATA FOR FILE 2)
[14]   ETC(COLLECTS DATA FOR FILE 3)
[15]   FCLUTCH 1 2 3 4
[16]   ((FREAD 1 F 529147),EN,(FSIZE 2
       529147)[2]) FREPLACE 1 F 529147
[17]   INPUT2 FAPPEND 2 529147
[18]   INPUT3 FAPPEND 3 529147
[19]   ⍳0 FAPPEND 4 529147
[20]   FUNCLUTCH 1 2 3 4
[21]   'MORE (Y OR N)?'
[22]   →5 IF 'Y'=⍞
[23]   DIRECTORY FUNTIE 1
[24]   ALPHA FUNTIE 2
[25]   NUMERIC FUNTIE 3
[26]   SCHEDULE FUNTIE 4
     ∇
```

WORD IS SUBROUTINE USED TO AVOID TEACHING APL NOTATION.

Explanation of *NEWEMPLOYEE* Program

[1][2][3][4] The file names *DIRECTORY*, *ALPHA*, *NUMERIC* *SCHEDULE* are tied to the numbers 1,2,3,4 for this user for the duration of the update after which they are untied in lines [23][24][25][26].

[5] The user is asked to enter the employee number.

[6] The employee number is stored as *EN* and split into the first two digits *F*, and the last three *L*.

[7] The *F*th component of the *DIRECTORY* is read and a search made for an element *L*.If it is found

[8] the employee number has already been assigned and a message is printed to this effect. Otherwise line [9] is executed.

[9]-[14] The user is asked for the *NAME* etc. and the answer is stored in *INPUT*2. This procedure is repeated until all data is collected for files 2 and 3. Note, the user will not be expected to provide scheduling data at this stage.

[15] *FSIZE* finds the component number of the next vacant component in file 2 (and hence 3 and 4). This number and the employee number, *EN*, are catenated to the existing directory data in file 1 and component *F* and the whole string of data is used to *FREPLACE* the previous string in directory file 1 component *F*.

[16]-[20] It is imperative that the correlation between component numbers is not lost. In the event that two people may be permitted to append to files 1,2,3, and 4, one append must be entirely completed before the next is started. The clutch operation picks up files 1,2,3, and 4 as they become free and then precludes access to any other user until the unclutch operation in line [20]. The whole clutch and unclutch sequence would only take a fraction of a second.
A blank entry is placed in file 4.

[21]-[26] The user is asked if he wishes to enter more data. If he does line [22] returns him to line [5]. Otherwise the program closes by an untie operation on files 1 to 4.

The third program *EXEMPLOYEE* permits the assistant to drop the record of an exemployee. It may contain a series of statements to check that the employee left over 2 years ago.

```
[N]→(TODAYS DATE-2 YEARS)>(FREAD 3 N 529147)[6]/(N+2)
[N+1]→0,ρ⎕←NAME;'EMPLOYED WITHIN THE LAST TWO YEARS'
```

The program will not allow the data to be removed except under the defined circumstances and gives an error message if the test line [*N*] fails.

Members of the accounting staff are required to renew their authorization regularly. This may be accomplished in one of two ways. An unlocked copy of the access function, stored under the protection of the file designers sign on password and workspace password, would be updated with new access codes, then locked and given to the user. Alternatively, the original access function could call on a fifth file for the expiry date. This locked program would only be able to *FREAD* the expiry date while a locked function owned by the Accounting Manager gives him the ability to *FREPLACE* the expiry date in file 5.

```
∇ AUTHORIZATION
[1]  AUTH FTIE 5 45678
[2]  'NAMES?'
[3]  L←(NAMES←⍞) LOCATE FREAD 5 1 45678
[4]  'NEW DATES?'
[5]  ((FREAD 5 2 45678)[L]←⎕) FREPLACE 5 2 45678
∇
```

(No attempt has been made to elaborate on the error messages or simplify the input of dates, which should obviously be done for a working function.)

After the tie function in line 1, line 2 asks for the names of individuals whose authorization is to be updated. Line 3 finds the index sequence of the names which is used to update the vector of corresponding dates entered in line 5 which are stored in component 2 of file 5.

The Line Manager is given access to all data on his staff. The Personnel department are responsible for keeping the department numbers up to date in the file system and the file designer may well cause a directory of names by department to be available to ensure that searches by department are efficient.

Hence the Line Managers will have a set of access programs which check their request against the directory of their employees.

And of course, each employee could be given permission to read his and only his file at any time so that he has a chance to see discrepancies or check his work progress against his commitment.

Summary

The complimentary attributes of APL and the Shared File System result in a fully interactive, time shared, remote terminal system, suitable for personal directories, historical files and shared files, retaining a high degree of file integrity and security.

The attributes of APL which contribute to the system characteristics include; powerful array operators which cannot modify or read themselves, locked functions which cannot be examined, locked workspaces for storing unlocked access programs, sign on numbers with passwords that can be changed at any time, and the fully interactive features of the language.

The attributes of the Shared File System which contribute to the system characteristics include; a set of new primitive commands to form files of unlimited size which are designed for shared file use, file authorization via access codes associated with primitive commands which link a user sign on number with a specified file's contents, primitive commands which can look at and modify authorization tables, and an ability to log unauthorized file access attempts.

Acknowledgement

The author wishes to express his gratitude for the assistance and suggestions offered by Larry Breed of the Scientific Time Sharing Corporation and by Ted McDorman and Ian Sharp of I.P. Sharp Associates. It is interesting to note that K.E. Iverson's son Eric Iverson, of I.P. Sharp Associates, played a major role in the implementation of the Shared File System. APL was first defined by K.E. Iverson in A Programming Language (Wiley, 1962).

CONFERENCE ON COMPUTERS, PRIVACY AND FREEDOM OF ... -- [POSITION AND BACKGROUND PAPERS].