PRIVACY IN VIDEOTEX

A

WORKSHOP

CONDUCTED

MARCH 12, 1981

VANCOUVER

SUMMARY REPORT

DRAFT

NOT FOR DISTRIBUTION

P. J. Booth

GROUP WEST

March, 1981

PRIVACY IN VIDEOTEX

A

WORKSHOP

CONDUCTED

MARCH 12, 1981

VANCOUVER

SUMMARY REPORT

P. J. Booth
GROUP WEST

March, 1981

PRIVACY IN VIDEOTEX

A

WORKSHOP

CONDUCTED

MARCH 12, 1981

VANCOUVER

SUMMARY REPORT

Prepared for the Canadian Videotex Consultative Committee
Sub-Committee on the Effects of Videotex on the
Individual and Society under Contract
to the Department of Communications.

This is a draft report and should not be copied or released for distribution without the consent of the Department of Communications and the CVCC Sub-Committee.

May 1981

P. J. Booth
GROUP WEST
March, 1981

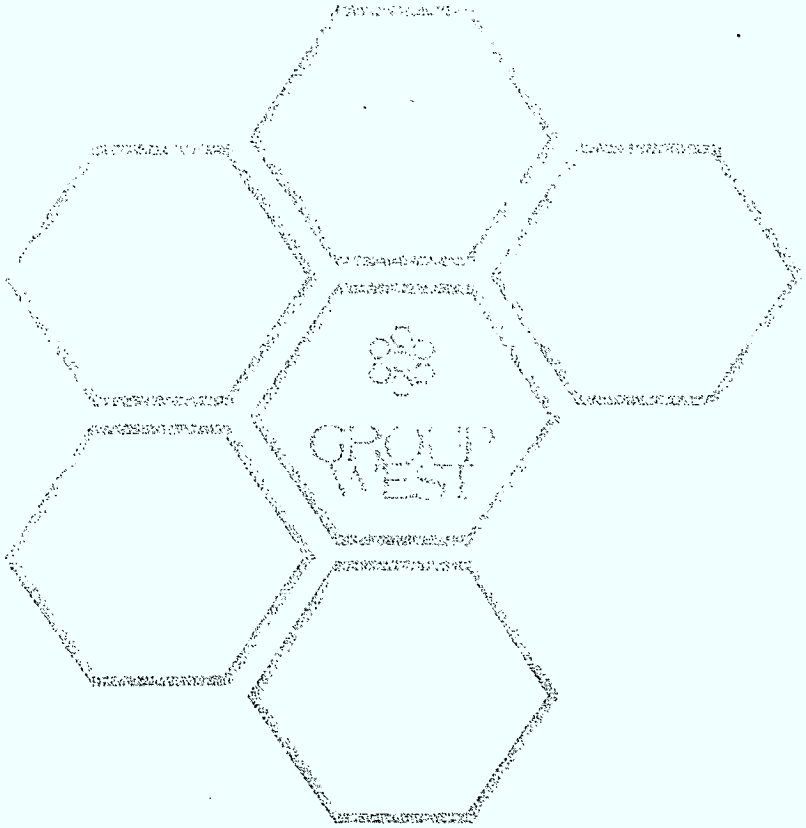
ACKNOWLEDGMENT

The author would like to thank all those people who participated in the workshop. As well, the input of Dorothy Phillips and Anne Cameron was greatly appreciated.

PREFACE

This report presents the results of a workshop conducted on behalf of the federal department of communications dealing with privacy and Videotex. The report is structured in the following manner. The first seciton provides the highlights of the procedings of the workshop. The next section provides a background to the development of Videotex services and presents a brief overview of technical developments. The subsequent sections discuss the issue of technological assessment and presents a brief philosophical and theoretical overview of the need for understanding technology and man in a humanist perspective. The major issues most directly related to the issue of privacy are then reviewed. The final section of the report presents the proceedings of the workshop. First an overview of the particular issue is presented along with an abridged version of each workshop presentation. The key areas of discussion resulting from that presentation are then provided. The attachments to the report include background material, the workshop agenda and papers prepared prior to the workshop.

TABLE OF CONTENTS


GROUP
WEST

OVERVIEW

1. The concern for Videotex should not be considered separate from the broader field of data communications, data banks and information acquisition. Videotex systems are viewed as a subset of the developments taking place, generally, in the area of data communications. They are also viewed as only one of a number of ways of providing information services and data communications.

2. Privacy was considered to be a fundamental right of individuals and something which should be assured for all individuals involved with electronic data communications. The proliferation of systems and the facility for developing large data banks with interlinking capabilities was viewed, under existing structures, to represent a threat to personal freedom. Privacy, freedom, autonomy and security were all considered fundamental human needs which should be respected in the development of new communication systems.

3. The protection of privacy and individual freedoms can be enhanced through the development of a variety of system configurations for Videotex. There should be encouragement for the small scale as well as large centralized Videotex operations. Control of information, provided and collected, should not rest in the hands of a few large IP's. Encouragement of special user groups and open access to the system was viewed as necessary to avoid manipulation and covert uses of information and user files.

4. Procedures need to be developed which limit the possibility of linking user data files for purposes not germane to the operation of a Videotex system or to the public good. Where secondary uses of data will be made, full disclosure to the user should be encouraged. Individuals should be given the right to opt out of such systems and not be subject to unknown or covert investigations of personal files.

5. The public should be made aware of the potential for monitoring user files in Videotex systems. As well, the potential for using such systems in alternative formats should be made known.

6. The consideration of information as a saleable commodity creates a situation which can limit intellectual content and freedom of information. This is particularly the case where a limited number of IP's control content. There is a need to encourage a variety of data bases and information providers and to foster access to such information. The freedom to access information represents an expression of human choice which enhances individual autonomy.

7. The legal remedies relating to privacy are ill-defined in relation to information data banks and data communications. The areas of relevance include:

a. Federal Human Rights Legislation
b. Freedom of Information
c. Contract Law
   - Breach of Contract
   - Breach of Trust
   - Breach of Confidence
d. Criminal Law
   - Liable, Slander

The history of cases involving contract law and areas such as liable or slander indicate difficulty in proving intent and quantifying damages.

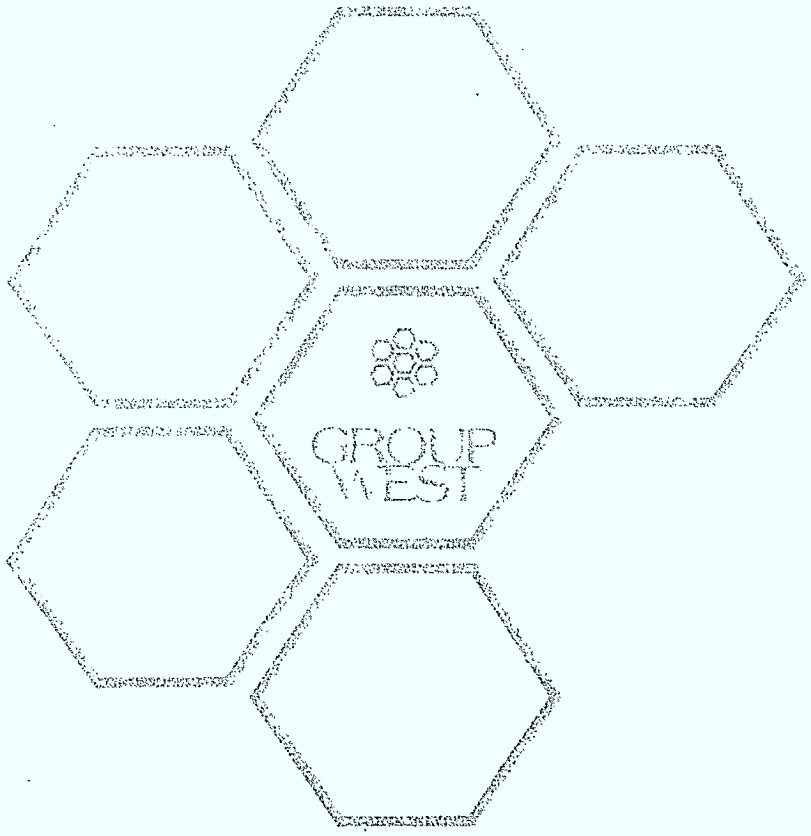
While ideally specific legislation for data communication and individual rights seems appealing, there are distinct problems in developing such laws. The rapid change in the technology and the obvious problems of enforcement are two key issues. Legislation seems to be rather vague and particularly ill-defined in cases of information use and the infringement of

human rights. This was evident in areas such as medical records and employment history.

8. Regulation dealing with the issues of security, privacy, disclosure, standards and data handling is a pressing need. The development of regulation should take account of the current system configuration as well as future configurations with encouragement of competition in system provision.

9. A key to inhibiting invasion of privacy would be the encouragement of open access to Videotex systems and an equitable distribution in system networks with maximum interconnection capabilities.

10. The protection of human freedoms and rights, including privacy, can be enhanced with the incorporation of consumer advocacy groups into the planning and policy development phase of system developments.


GROUP
WEST

SECTION I DEVELOPMENT OF VIDEOTEX

There is a general agreement among philosphers, scientists and researchers that in the field of communication, our society is currently in the process of a major revolution. This revolution is signifying the movement towards a society which is becoming increasingly polarized around the production, collection, transmission and processing of information. It is a society which is increasingly dependent on information to facilitate the functions of exchange, development and human interaction.

There has been, and continues to be, a substantial growth in the development and diffusion in our society of a whole family of communicating devices. This has been most rapid over the past ten years. While the initial significant developments occurred in the telephone market, most recent periods have seen a coincident growth of computer data communications.

In the past few years, the technology of communications has proceeded at an accelerating rate, producing new services and expanding the capabilities of existing ones. The present sees a general merging of the boundaries between the various modes of communication. Classification of those modes presents essentially four types:

A.	Broadcast	-	T.V. Radio	-	Computers
B.	Satellite	-	Special Networks	-	Computers
C.	Telephone Lines	-	Telephone	-	Telex/Computers

D. Cable - Pay T.V. - Computers

Each of these types has associated with it a specific communication device or service, the most well known being television, computers and the telephone. Each of these currently interact to provide the networks which exist for the delivery of information and to facilitate the flow of information in our society. A critical innovation in recent years has been the development of communication devices which are hybrids of the more traditional modes. In particular, the expansion of computer technology and the creation of micro-processing has revolutionized the communication industry. Two technological developments which play a significant role in the changing nature of communication are the miniaturization of electronics achieved by the increasingly complex circuitry of semi-conductor chips and the proliferation of cable T.V., satellite transmitters, digital networks and optic fibres. The first has resulted in an astonishing reduction in both size and cost of electronic devices. The second development seems likely to assure that sending and sharing data will continue to become simpler and faster, and especially significant, the costs will become independent of distance.

The devices which have resulted from these changes in technology and information delivery are smaller and more versatile computers. Within the past few years, personal computers have been quite common and their diffusion has been quite rapid. However, another family of devices has developed which utilizes existing networks for delivery and provides access to information,

processing and interaction between various small computers. These have become known by a variety of generic names, but may best be referred to as an information utility.

The merging of computers and telecommunications and the ability to provide ubiquitous information access and interactive capability has resulted from several basic technological developments. Micro-electronics development of the integrated circuit has progressed steadily since 1960 to the point where a single silicon chip can provide the number of components previously available in the large computer. Each individual silicon chip, less than one quarter inch square, is the equivalent of a small computer capable of executing about a million instructions per second. The critical elements in this technology have been the vast reduction in costs for processors and the increased capability for processing. In the telecommunications industry, dramatic advances have been made. These are essentially in the areas of transmission and switching. New channels for transmission have vastly expanded the capacity of communication networks. Today there is simultaneous voice, video and high speed computer data on a single line. Critical to this is the use of co-axial cable, microwave, satellite transmission and optic fibres. Changes have occurred in the amount and quality of information carried by the various devices, and as well in the extent of coverage for communication.

Another important technological change has been the shift from analogue to digital transmission. Analogue represents the steady flow of signals along

independent bands. Digital allows messages to be sampled periodically over a very short time and the bit streams of many messages are interleaved (multiplexed) and sent along the same line. This advance maximizes the use of a particular line, thereby increasing the flow of information and providing the high quality of transmission essential to computer data flows.

Two other developments which are critical to the advances in communications are the growth of computerized telephone exchanges and the use of packet switching. Each has enabled the expansion of the flow of information, and as well as the spread of advanced technologies requiring the most advanced network capabilities. These developments have been instumental in facilitating the growth and expansion of communication services as an integral part of our society. The telephone, computer and other forms of communicating devices have all benefited from these services.

The main development of relevance to this study has been the capability for information utilities. There are, it should be pointed out, a number of these services currently developed and in use within Europe and North America. These may best be described first in terms of the basic hardware which is common, and secondly, in terms of a specific service developed in Canada.

The basic hardware consists of:

A. A programmable, central processing unit

B. Memory device

- Semi-conductor fast memory
- Magnetic tape cassettes
- Large volume memory
- Videotapes

C. Input Devices

- A keyboard
- A voice activated device for transforming a limited speed vocabulary into recognizable machine signals
- A credit card reader with appropriate guards
- Pen-device for graphic capabilities
- A marking tablet

D. Output Device

- Television screen
- Copy printer
- Speaker

E. Communication Channels

- Cable to television networks
- Telephone to public switched systems

Telidon is the name of the Videotex system developed in the Canadian Department of Communications. This is a device which has the hardware characteristics described above, but which also includes the technology for graphic and textual display of information. The system is considered an inexpensive means of providing access to information by means of a modified

television set. The ultimate goal of a Videotex system is to enable a user to access virtually any information from his/her own home. The system operates through a network to a central computer, whereby the user can access information and obtain responses. Telidon uses ordinary telephone lines connected to a host computer. Each user is equipped with a terminal and a key-pad and would be capable of using that key-pad for selection of a range of information. The Telidon terminal contains sufficient intelligence and memory to enable it to be configured to act like a stand-alone computer and to execute programs that have been downloaded from a remote computer.

The possible uses for Telidon include:

A. Information access and retrieval (generally)

B. Education and computer assisted learning

C. Entertainment

D. Travel reservations

E. News

F. Transactions, ie: Credit shopping, banking, libraries

G. Home utility monitoring

Basic research and development into new interactive visual communication systems commenced at the Communication Research Centre of the Canadian Department of Comunications in 1969. From 1969 to 1973, considerable effort went into building special hardware and in producing the necessary software to establish a capability in interactive graphic communications. This led to the

development of an interactive programming language (IGPL), and later to the initial definition of the Picture Description Instructions (PDI's).

From 1973 to 1979, the hardware (display processor unit) and PDI communications protocols were refined, where the basic philosophy was to require that the terminal would contain its own intelligence (micro-processor and display processor) and that the picture coding scheme would utilize that fact. The Canadian Videotex System - Telidon was announced in August 1978, and further refinement of the terminal has progressed since that date.

SECTION II ASSESSING VIDEOTEX - THE CRITICAL ISSUES

The development of computer linked telecommunications devices such as Videotex or Telidon has opened the door to numerous discussions relating to the macro and micro issues inherent in its development, and to society's acceptance of that innovation. Issues are now being raised which address the concerns of social policy, regulation and legislation. This has been manifest in the realization of the need for the development of government policy with respect to the processing, handling, storing, carriage and brokerage of information generated by computers generally and Videotex in particular. There is no doubt that issues relating to the development of this service are current, and highly relevant to the data communications industry and society in general. Areas which require further investigation, or at the least consideration, are current regulation, existing legislation, social policy, technological capabilities, standards and societal norms or expectations.

Speculation about the direction this new innovation will take and its consequent effects have been made by numerous researchers and industry practitioners. These range from the optimistic views of the futurists with visions of wired cities, electronically managed living environments and spatially altered landscapes to the pessimistic views of psychologists about the inherent dangers of alienation and the desocializing effects resulting from the reduction of face to face contacts. Others have raised the issues of centralized information control, and the spectre of an Orwellian society where individual rights and

freedoms are minimized and automony ceases to be possible. In such a society the individual is controlled by the machine and those in positions of power reach out and influence the citizen through the technology.

The divergent opinions about Videotex are often difficult to reconcile and to forge into a coherent scenario for future developments. There is, it seems, no denying how engaging the technology seems to be. There is a blend of innovativeness and appealing application which can meet some very gratifying ideals for managing society. Such innovations aid in bridging the gap between the physical elements of human behavior and existence and the nosphere or knowledge sphere of human thought. The reality of the present state of development requires the consideration of those elements which will, to a great extent, influence the ability of society to adapt to these innovations and the capability of individuals to alter their behavior to perceive such innovations as effective and useful tools for everyday life. The infrastructures which are developed and the institutional frameworks which are set up are an integral part of the orderly development of such a technology. Fundamental to that process is a need to minimize the negative impacts resulting from the innovation on individuals and society.

Ellul (1964) has elicited similar concerns in a philosophical context by stating the need for an understanding of the humanist perspective in a rapidly accelerating technological world. A critical element is the need for bringing technology and man together in the development stages of an innovation, rather than juxtaposing

one against the other in the production and operational stages. In a rather Hegalian or dialectic view, the two elements should be considered equally important and closely linked to ensure an equitable development with the minimization of negative effects on society.

PRIVACY & DATA COMMUNICATIONS

In 1971, the Department of Communications and the Department of Justice issued a report on Privacy and Computers. That report was part of the Task Force on Computer Communications set up to aid in ensuring the orderly development of communications in Canada. The Department of Communications was interested in two issues:

- Assessing the probable consequences of current and future communications technology.
- Identifying the social and economic needs which might be met by communication systems.

The advent of Telidon and the range of services broadly defined as Videotex has created a renewed interest in the issues focusing on the social consequences of computer services. A central focus of that concern is the issue of the social and psychological impact of Videotex on the individual and society. Within that broad paradigm, the issue of privacy represents a central focus. Privacy issues have been identified in two contexts:

- Primary uses of data; banking, messaging

- Secondary uses of data; billing records, access, tracking

In previous studies dealing with privacy and computers, the D.O.C. Task Force (1975) outlined the criteria needed to minimize threats to individual rights:

"It must provide security and protection of privacy in the areas

of: data acquisition

data storage

data dissemination"

In the areas of acquisition, all information relating to the individual must be sanctioned by the subject, him or herself, except where such information is seen to be of importance to the public, i.e., police records. The subject must have access to the data acquired for verification, be advised of how and by whom the data was acquired and how they may be used. Furthermore, those authorized to collect data must be bound by legal and professional constraints in what data they collect and how it is collected.

In the area of data storage, methods by which mechanical and human error may be identified must be devised. Provision must be made for the updating and purging of data by personnel bound by legal and professional constraints. The very quality of storage must be assessed to ensure the data is protected from deterioration or illicit access.

In the area of data dissemination, the owner/subject must be identified and given access to verify data and sanction item sharing. The reliability of all data and computer analysis should be assured before dissemination.

An overriding need for data communications is the development of legislation to enact laws which protect the rights of individuals and which codify the precedures outlined. For the development of the legislation, standards of performance must be defined along with a realistic assessment of enactment and enforcement. There are as well major problems of jurisdiction and definition which need to be addressed.

PRIVACY & VIDEOTEX

This evaluation of the concerns relating to Privacy and Videotex is designed to address a range of issues relevant to the individual and society generally. In Gotleib's (1978) review of the effects of computers in the home, a critical impact was identified as access to information control and security. It was suggested that the most significant problems for this innovation will be:

- Jurisdiction
- Licensing
- Content

In discussing the public acceptance of the service, privacy was identified as a major issue:

> "Will questions about confidentiality and privacy, and doubts about changes in lifestyle add to the concerns of a public that is increasingly unsure about the enveloping influence of computers" (Gotleib, 1978, p. 25).

Cardell (1975), in assessing the impact of computers on society, suggested that we are at a critical stage where a number of important decisions will be made on how technological innovations develop. An overriding concern was specified as the degree to which man as social being can achieve full control over his own life situation. In maintaining privacy, the fundamental concern rests on preserving individual freedoms and fostering the development of new technologies in such a way that they contribute to the realization of positive social goals. Failure to do so, it is suggested, may lead to a further isolation and powerlessness which too many people already experience in society.

The issue of privacy has also been raised by Gardiner (1980) in his discussion of Data Banks and Personal Automony. In that discussion, Gardiner examines the issue of privacy at the individual level and considers issues from a psychological perspective. A fundamental point is the distinction between privacy or loss of privacy and the erosion of automony. The basis of Gardiner's distinction lies in what he refers to as the degree of control individuals have with respect to the accumulation and dissemination of information. In a sense, that control represents the degree of self-determination an individual has with respect to data which may be used to gain knowledge about him or herself by other individuals. It is the loss of that control which represents according to Gardiner,

the threat to the individual so inherent in the accumulation of central data banks.

In assessing Gardiner's viewpoint, two important concerns become evident. One is the types of data individuals disclose about themselves in various societal transactions. Such transactions are, for example, an application for credit or the accumulation of data under a SIN number. Second is the secondary use of such data and the facility for cross referencing data sets to form profiles. Common thought tends to view the second point as the fundamental evil. Gardiner's view is that the creation of central data banks equate to a loss of personal automomy, and hence facilitates the invasion of privacy. However, just as Gardiner illustrates that Privacy is a relative term, so too must issues of automony and control must be viewed relatively. The issues of societal norms and expectations be examined to illustrate the extent to which individuals feel a loss of automony. Clearly in many minds, living in a technological society requires the acceptance of a certain degree of impact on lifestyles and freedom of choice. The important issue, however, may be the assessment of where on the continuum between the total loss of automony and a pristine world of full self disclosure our society will develop. As well, the need exists to ensure that whatever degree of personal rights and self determination are considered acceptable, they are equitable for all members of society.

Other issues relating to privacy have also been raised. These touch on the structures necessary to provide equitable service, the legal remedies and

interpretations of privacy, as well as the methods for insuring individual rights and protecting human freedoms.

BIBLIOGRAPHY

Department of Communications. Telidon Aggregated Statistics. Department of Communications/Government of Canada, July 1980 - Ottawa.

Ellul, Jaques. The Technological Society. Vintage Books, Random House, N.Y. 1964.

Gardiner, S. Personal Data Banks and Personal Autonomy. Science Council of Canada, Ottawa, 1980.

Gotleib, C.C. Computers in the Home. What Can They Do for Us - And to Us. Institute for Research on Public Policy, Ottawa, 1978.

Halina, Jos. W. Communications and Communities. A North American Perspective. International Commission for the Study of Communications Problems - Unesco, 1978.

Jordan, F.J.E. Privacy Computer Data Banks. Communications and the Constitution. Privacy and Computer Task Force - Ottawa, 1975.

Pergler, P. The Automated Citizen. Institute for Research on Public Policy - Montreal, 1980.

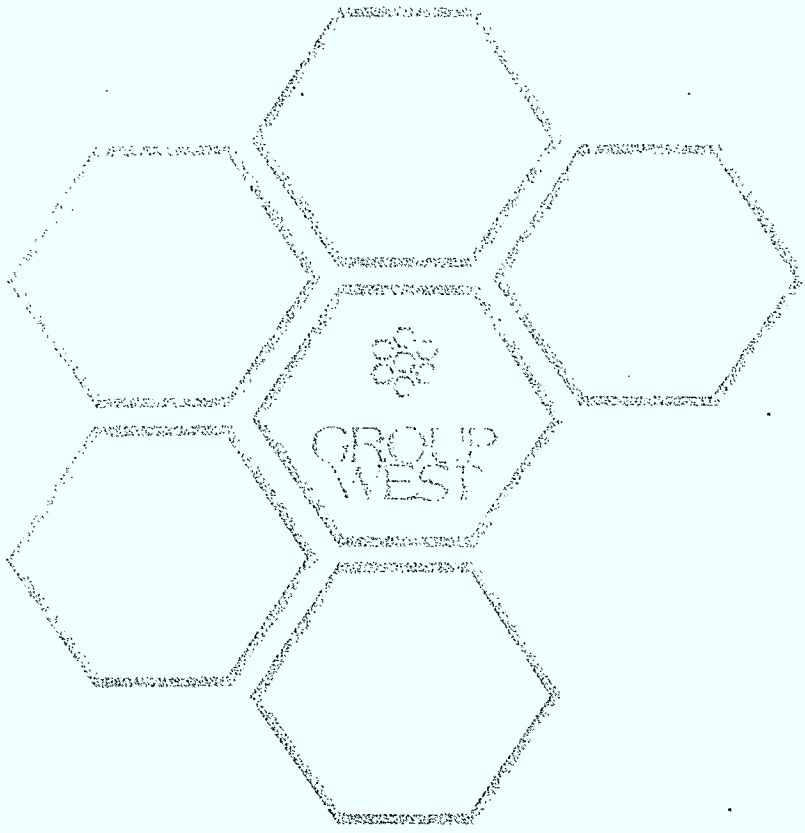
Plowright, T. Social Aspects of Videotex Services. Proposed Research Directions. Social and New Policy Division, Broadcasting and Social Policy - Federal Government of Canada - Ottawa, 1980.

Royal Society. Communications into the Home. Royal Society of Canada, Ottawa, Canada, 1972.

Secretariat for the Future. Man in the Communications System of the Future. Stockholm, Sweden, 1975.

Sharp, J.M. Regulatory Models. A Study for the Privacy and Computers Task Force. Department of Communications, 1975.

VISPAC. Draft Code of Ethics. Videotex Information Providers Association of Canada. Ottawa, 1980.


GROUP
WEST

SECTION III WORKSHOP PROCEEDINGS

As a first step in the assessment of the impact of new technologies, such as Videotex on the individual, the Department of Communications sponsored a workshop. The purpose of the workshop was defined as:

> An investigation of the impact of the development of a new technology such as Videotex on the individual rights and freedoms with particular emphasis on the issue of privacy.

The workshop was designed to examine privacy in relation to:

1. The concept of privacy and the individual.

2. Primary data acquisition:
   a. Gathering and using such informtion.
   b. Processing and storing information.

3. Secondary data acquisition:
   a. Disseminating private information.
   b. Protecting individual rights.

The concept of privacy and the individual was examined in terms of how people feel about privacy. This was based on the moral and ethical issues of privacy. As well, the concept of privacy was addressed from a socio-psychological perspective.

The primary data acquisition phase and gathering of private information focused on how the systems could be designed to protect privacy. This examined system architecture as well as the alternative structures which could be manifest for providing such services. Other issues included the ownership of information once it was gathered.

The secondary data acquisition and disseminating of private information focused on several items. These included the legal aspects of privacy, the use of data once it is gathered, the selling of information and the method for ensuring anonymity of individual records.

Other issues dealt with the agencies monitoring services and the protection of privacy for those individuals whose records are stored in a system.

FORMAT

The workshop was held in Vancouver on March 12, 1981. Fifteen individuals were invited to the session, either as key speakers or as participants. As well, a number of observers attended the session. There were nine speakers, each addressing a particular issue within one of the four main areas of investigation. Individuals were selected based on either their knowledge of Videotex or because of a special interest related to Videotex. Representation was made from:

- Religious Community
- Acedamics
- Research and Consulting
- System Designers
- System Providers
- Information Providers
- Citizen Advocates
- Legal Community

The proceedings were structured to allow individuals a thirty to forty minute presentation. At the conclusion of the presentations, the chairman allowed discussion from the floor.

This report presents a summary of the workshop proceedings along with the responses to the various presentations. In each section, an overview of the discussed issue is made. The basic text of each presentation is also included in this review of proceedings.

OBJECTIVES

The objectives of the workshop include:

1. To bring together professionals who are involved as well as interested in the issue of privacy in the information society. To provide a forum for the exchange of information and the development of opinions on that topic.

2. To examine the definitions of privacy and to consider the concepts of privacy and autonomy.

3. To consider the possibility and consequences of a concomitant rise in public resistance to private information storage.

4. To discuss how data might be secured and be seen to be secured.

5. To examine the ownership of information, the legal aspects of data communication, its control and regulation. To discuss the jurisdictions under which these controls should operate.

6. To examine the institutional and operational arrangements which are viable for the provision of a variety of system configuration for Videotex.

PROCEEDINGS

1. PRIVACY AND THE INDIVIDUAL

The discussion of privacy was initially presented in a moral, Christian philosophical context. The basis for that approach rested on human freedom. The fundamental question was whether innovations, such as Videotex, can violate or impinge upon human freedom. That was discussed more specifically in terms of:

a. Personal or civil liberty.
b. Unrestricted access.
c. Responsibility.
d. The right of autonomous action.

NEIL HUNTER

PRIVACY AND THE INDIVIDUAL

Thank you very much, Mr. Chairman. I'm still not exactly certain whether I'm at the right place. It's just been really incredible to observe. To come into a situation like this--nobody, except for _____ and _____ that I know and just hear the jargon coming out and I have an awful feeling that what I will end up doing is throwing a lot of jargon that comes out of my thought form and my framework, and I hope I don't do that. What I'm really hoping I'm able to do is even touch base somewhere in the ball park where I think we may or may not be today.

Anyhow, if you look at the way I've been described, you have to appreciate that I guess my initial starting point is to introduce my comments as a Christian; therefore as a person who attempts, when raising questions and looking at perspectives, to not only think of them in terms of the cultural and the sociological and the social and intellectual, and all of these components, but also a theological component, which is, in my point of view, not unimportant and, in

terms of the way I think and operate, it ends up being the first question and ultimately ends up being the last question, too. So the kind of thing that I keep raising in my perspective is: what is it that God wants people to do and be? What kind of ideal world ought we to be looking at, trying to understand and trying to create, or co-create as the word may be? As a Christian I attempt to keep my eyes open and my ears open and to read and to listen and to try and understand and weigh all these things against the historical perspective of the Christian church and to address the broad concept, as I understand it, along with the teachings of the prophets and the New Testament teaching. What I really want to say, then, is to try and narrow down in one area. I think the area I want to address myself to is the area of human freedom and whether or not the whole possibility of privacy in videotex somehow violates, or at least impinges upon, human freedom. In the Gospel of John, Chapter 8, verse 32, Jesus says "You shall know the truth, and the truth shall make you free" - probably one of those quotes that people have heard from time to time, and used properly at times and improperly at other times. The difficulty with putting a quote like that in front of us is that obviously we hit two philosopical problems. What do we mean by truth and what do we mean by freedom? I'm not going to spend much time trying to address those, although I realize that they certainly raise more questions than they answer. To simply say that, in my opinion, religion as a pursuit, as a component of one's life, essentially addresses itself to a quest for truth: to try to understand reality in its ultimate and final sense. To paraphrase one of the well-known 20th Century theologians, Paul Tillich, "religion is ultimate concern". It seems to me when one reads religious material and the scriptures of any religion in general, one ultimately sees that the direction in which religion has to move in a progressive sense is towards a sense of freedom. Freedom in the sense of personal or civil liberty. Freedom in the sense of right or personal choice or action or thought. Freedom in the sense of unrestricted access--restricted only by the commensurate sense of responsibility, because always in theology, wherever you have one thing that you talk about, there is always the counterbalance of principle which is probably true in other businesses too. When we talk about freedom, we must see it in terms of some kind of responsibility.

Freedom, then, and I come to Mr. Gardiner's expression that he uses in his paper, freedom is the right of autonomous action. The right, inalienable right I suppose, the civil right, for me to make autonomous, intelligent, informed decisions without being restricted or impinged upon by forces which are beyond my control. If we do a very quick kind of historic overview in terms of the whole kind of movement of the monotheistic god in society, you can understand that the most important event in the Old Testament is the Exodus. This is seen as the freeing of the slaves from Egypt by a being known as Gaweh (?) or God, who acts volitionally of his own or her own volition, to take a people who are not free, who were not able to make their own choices and decisions and to move from the situation and give them that sense of freedom. There is that kind of exodus motif that runs through virtually every book in the Old Testament and is picked up and followed very much in the New Testament, and also is seen as Jesus of Nazareth being the instigator of the second Exodus: the act of freeing humanity. Not so much the second time in terms of freeing from oppression by another nation, but freeing in the sense of freedom from guilt, be it either self-induced guilt or guilt put on by external sources.

That which restricts freedom always will remain a very big religious question. I don't know whether there are any historians in the crowd--if there are, then I'm in trouble--but let me continue. It seems to me that the Inquisition, which tended to restrict freedom, produced an incredible reaction in the form of a whole new movement in Protestantism and Industrial Revolution which, as it came into being, tended to be non--it was amoral, there was no moral component, but after a while the abuses of the Industrial Revolution produced a whole new question about human freedom in terms of the coming of the Machine Age, and once again, the theological questions had to be asked about how we interact in our environment with whatever technology we have. The whole question of El Salvador today is a question of human freedom, and the kind of horrendous political fall-out which is happening and which will continue to happen, is the whole struggle of how a group of people who want some control over their own resources and over their own lives deal with the super-powers and other political social realities.

We would say that the ultimate truth is that God created man or man comes in to his own being to be free and to be responsible. I don't personally believe the story of Cain and Abel as a historical story, but it certainly is a parable or lesson about one's freedom versus one's responsibility to one's neighbour. Am I my brother's keeper? The answer that one must--the answer is invariably yes. The question of freedom, I think, is really prevalent in today's society.
We have Women's Liberation, we have Human Liberation, we have the kinds of things that are happening in Chile and Nicaragua and Campuccia, minority groups, we have gays coming out of the closet, so to speak, and asking for their rights. So I suppose the first question I want to raise is to what extent does the whole technology of videotex which--I guess I have to raise a very dumb question--videotex to me seems to be one of those book words, and I'm not sure that I really pick up on it, so if it sounds like I don't pick up on it, it's because I'm not sure that I've really come to grips with the terminology that's familiar to you but not to me.

But anyhow, my one question is to what extent does Videotex and databanking impinge upon or suppress freedom? Freedom to opt out of the system? One of the quotes that Mr. Gardiner used, and I hope I'm stealing all of his information, but something to the effect that if something looks like it could be used, we should use it. In other words, there's a kind of a wave that sort of rolls over all of us and to what extent does that wave that rolls over all of us--we're all plugged into the computer whether we like it or not--impinge upon this idea of freedom? Freedom to withhold information. Freedom of our privacy, of thinking that there are two kinds of information--public information and private information. Another question I raise that comes out of this is simply the amount of information available to the public. When I listen to Mr. Godfrey talk, and you'll probably hear him later on this morning, once again, I think we here are talking about something that, in my opinion, about 95% of the population knows absolutely nothing about. I don't want to raise questions like conspiracy, but I personally begin to get a little paranoid in a situation like this. Something is happening, something rather vague, something that people are either uninformed, or misinformed about, and I wonder about that. Most lay people - and I'm a lay person when it comes to the electronic revolution - know nothing

about electronic technology. They know nothing about the collecting and the storage and the retrieval and the dissemination of data in terms of databank. So I raise that as a question. Just how up front and how candid are the people who are bringing this into being and maybe we can't even talk about people who are bringing it into being, but there seems to be a lack of candidness about the whole thing to me that, ultimately, is freedom-denying. It reminds me of that quote that was used, once again, in a novel by the Tomorrow File, which says "you have no need to know". And I guess what I'm saying is the people have a right to know. On the questions of human freedom, which is really where I'm coming down in terms of my theology perspective, the question of conformity versus uniformity or individuality. Is it necessary in the modern world to give up certain rights in order to expedite what the general population or some of the population thinks to be good or new or better, and therefore by definition, necessary? For example, every time my wife goes into The Bay and cashes a cheque, she is asked for her social insurance number, so she doesn't give them a battle, because she won't do it, you know. That's the kind of thing I mean, conformity versus individuality. Then this question of human freedom: is the whole technology such that the right of doubt is real or will it at some point not be a right at all? I guess one of the reasons I'm here is because _____ and I got talking about social insurance numbers, that's what I hang my whole situation on. That it really all started, if I can just share this briefly, when I and my wife, as parents in our community decided to join a block parent program started by the community school. It's administered by the R.C.M.P. and when you fill out the block parent program you're supposed to give your social insurance number. So I said I'm not going to do it, and they said phone the R.C.M.P. and tell them you're not going to do it, so I did, and they said why don't you want to do it? I said, well why do you want the number? It facilitates the security check. And I said, how does it facilitate the security check? He said, well, we have access with your number much faster, otherwise we have to go through a detailed, painstaking check. So I said, well then, you're going to have to go through a detailed, painstaking check. I'm not giving you my number. But the problem was that I was a suspect and I think they probably were trying to find out whether I've been to Russia recently or something like that, and I felt like a second-class citizen simply because I was opting for the right to not disclose at this point. The right

to opt out as an exercise of my human freedom as I understand it, without being suspect, is a very important question.

What information is private? What information is not germane to the matters at hand, and this is a terribly vague kind of statement and I think it needs more definition, and I'm not sure how to define it more clearly, other than to say it seems to me that the problem with electronic data collecting is its limitless. If we listen to the radio in the States, it's limited only by our imagination. I don't think that one's ideological, religious, political or sexual preference has any relationship at all to whether or not I qualify for a mortgage, yet it seems to me that the way one can take information and think of it in terms of exclusive information; does this person pass bad cheques, does this person maintain bank accounts, do they pay their bills regularly, sure that's important to a mortgage; what's their income, how can they afford to sustain the payments - that's important. But it seems to me this other is not germane--it simply doesn't answer the questions being asked, or, are we looking at a whole new way of asking questions; namely, all information is germane, even to the most mundane or highly narrow kind of questions. I don't know, but to me there's information which is public and there's information which is private, and private information--I suppose I'm working on a definition--is that which may not necessarily be germane or important or related in an organic or definitive way to the questions which are being asked.

There is the question - I'm not sure which paper it came from - which raises an interesting question that has probably more implications for the religious community than for any other. The question of what I call rehabilitation or recovery or forgiveness versus--I put here--a machine and a system that never forgets. Fundamental to the understanding of Christianity is that one's past is not held against one. That one can't start anew. It seems to me that if I pass a bad cheque in 1965, I may have to live with that in the databank wherever it might be for the rest of my life. So I question how does one go about screening information and how does one go about correcting it, how does one go about eliminating that which is not important or relevant, and how does a computer forgive?

I have trouble defining privacy, but I guess I'm saying privacy is that which is not open to public access. I guess I'm believing that there ought to be two streams of information and that probably what happens is that gap between the two is narrowing.

Just a couple more ethical questions, before I close down. The ethical question of whether one is innocent until proven guilty. The withholding of information--is that seen as a presumption of guilt? And a second question which is a very broad kind of ethical question and certainly, in my opinion, part of the fabric of the democratic institutions; namely, that the insitution and the state serve the people rather than vice versa. To quote from the Bible, "the Sabbath is made for man, not man for the Sabbath". I think institutions and technologies have to rise to respond to human need rather than coming out of the narrow perception of a certain kind of mindset and creating a whole new set of problems. And then we in the church keep thinking that there's some rather vague notions about right and wrong and it's awful hard to figure out what's right and what's wrong in the world any more. It's like a record that gets stuck in your head and keeps coming back to haunt you. Something just doesn't sit right and you can't figure out why but you have this notion coming out of an era when God was viewed far more objectively than today. There are certainly things which are fundamentally right and some things that are fundamentally wrong and so I have trouble with this. The problems of order versus anarchy, problem of whether or not there is a kind of an over-riding moral force in the universe within humanity that corresponds to a moral and just universe. And the last point, that there is justice and that, as a theologian and a Christian, God is the final arbiter on all matters.

Related to the discussion of these issues was the question of "what information is private?". That issue was very difficult to define. The view was expressed that the scope and extent of electronic data collection is limitless and thus allows data to be used which is often of only marginal relevance to a particular activity being undertaken. Information about an individual can be used to reveal characteristics which are often not germane to the purpose for which the information was originally collected.

A final area of discussion focused on the religious concept of forgiveness. On that point, the question was raised about the ability of computer data banks to "forgive". Where data is collected and stored, should there be some procedure for removing files about an individual after a set period of time?

The development of Videotex was viewed in the context of "responsibility" to society. It was suggested that such innovation should ensure that personal freedoms are not restricted but, rather, enhanced and that society should be given more and better access rather than being restricted and limited in their activities. There should be a right "not to provide information" at an individual's discretion.

The conclusions drawn from the moral perspective focused on the need to avoid restricting human freedoms. Through such a concern, the fundamental right to privacy for the individual would be maintained.

Discussion of the moral issues and questions of human freedoms was focused on the use of data to discriminate against people, either in their jobs, or personal life. Examples were provided about sex discrimination and the unknown uses of personal data files. Concerns were also expressed about the development of legislation and regulation since enforcement of such laws would be extremely difficult. Further, relying on regulation requires a great deal of trust between the information processor and those who give information for whatever purpose.

Suggestions were provided that a centralized regulatory body may not provide the best method for ensuring the protection of rights but that a decentralized structure would be more responsive.

The issues raised within the moral context included:

a. Freedom of individuals to opt out of the system.

b. Individuals to remove themselves from the system once they are involved.

c. Individual's right to withhold information.

d. Individual's right to know and be informed about information.

e. The surrender of individual rights.

f. The limitless nature of electronic data.

g. The need for re-evaluating societal norms with respect to the concept of private information.

h. The concern for the purging of information from a system.

The second area of discussion, relating to privacy and the individual, was directed to a socio-psychological interpretation. This was based on considering privacy in relation to autonomy.

SCOTT GARDINER

PRIVACY AND THE INDIVIDUAL

I understand that you have all read or at least received the first paper. Just a few preliminary, throat-clearing remarks by way of history of this paper, in order to get you acclimatized to the accent, before I say anything important. Arthur Cordell at the Science Council asked me if I would write a think-piece about the issue of identity and personal databanks. He assumed that the question of identity was a deeper issue lurking underneath the discussions of privacy. So this paper, then, was a response to Arthur's question about the question of identity. This was a third draft. I had presented it to Arthur as a preliminary version, but he accepted it as a final version. Probably very sensible, because I tend to compulsively work over and over a paper, not necessarily improving it in

the process. I once wrote an introductory text book which was successful enough to support me for a number of years and then I revised it and the sales went down so much that I had to go back to work. I'm now working on the third edition--I'll probably improve it out of print. However, in the interval since I submitted this third draft to Arthur, I do believe I've made some progress in thinking over this issue. So this paper is an attempt to, as I say, revisit the earlier verson, and outline the general skeleton of the argument and flesh out the parts which are new and beyond my thinking in the original paper.

The major thesis is that the primary concern is not so much the invasion of privacy as erosion of autonomy. And the argument is first of all that privacy is a relative concept whereas autonomy is an absolute concept. I've found it difficult to find a translation for privacy even in French. I certainly can't find a translation in Greek. It seems to be very much an Anglo-Saxon hang-up. It varies from individual to individual. Some of us have unlisted phone numbers, some of us carry pagers, but it all varies from culture to culture. In some third world countries, the bottom apartment on the street side is most expensive because they value conviviality over privacy. So it seems to be a very relative concept, whereas the concept of autonomy seems universal. It seems that the process of development, always filed genetically from animal to human, and ontogenetically from child to adult, is a process of progressive emancipation from the tyranny of environment. So autonomy seems to be something that is universal--built to our genetic program, a process of emancipating us of the tyranny of our environment, establishing autonomy with corresponding responsibility.

If you put a glass screen between an octopus and a crab you find that the automatic response of an octopus to a crab, is crab, crab, crab, crab, crab; but if you put a glass screen between them, then it's not able to do that. Apparently, the octopus is able to turn around, go around the glass screen, and get the crab that way. So apparently, then, its behaviour as it's turned away from the crab - going around the glass screen - must be guided by some image of the crab. So it's able, then, to delay its automatic response to the stimulus, crab, because it has within its mind, (this is the beginnning of the mind) it has some image of the

crab, so it's responding then not directly to the environment, but with respect to some image of the environment within its mind. That's what I mean by saying that we develop the capacity to not respond, that is, we're no longer at the mercy of our environment. That is, we can say no to our environment. That is, we can choose between different responses. So as you look through the philogenetic scale, or look through the ontogenetic scale, fifty years of work by John Piaget demonstrates that it is a process of development, and ontogenetic development is a matter of progressive emancipation from tyranny of the environment; in other words, developing the capacity for autonomous action. The central aspect of autonomous control over one's identity and that process of ontogenetic development is one of acquiring an identity and this personal identity is intimately tied to public identity. You may be familiar with the study of the Pygmalion classroom where Rosenthal and Jacobson found that by telling teachers that certain students were underachieving and were going to bloom next year, B students improved not only in their grades in class but in their I.Q. scores as a result of the expectations of the teacher and they called that the Pygmalion classroom after the Pygmalion character in the story. It seems from that research and a lot of research, that we're all, in many personal relationships with other people, supported by a net of expectations or entangled web, if you like, of expectations and we all have our Pygmalions who determine our personal identity by various expectations that they have of us. This is a two-way process because we present ourselves to people in a certain way which gives them certain expectations of us, which feed back to us. So we're involved then in a two-way interaction between our personal identity, our reputation with ourselves so to speak, and our public identity or reputation with other people.

Now this matter of the way in which we present ourselves to other people--there seems to be two very different views within psychology. There's the view that the person should make an open and honest presentation of themselves in public and that's Sidney Gerard's concept of self-exposure. The antithesis to that is a person should present themself as is appropriate to each situation and that is most intimately identified with the Impression Management theory of Groffman. I'm attempting some sort of synthesis of those two points of view by saying that the important thing is that the person should be free to disclose himself to some

people and manage their impression with other people as he or she wishes. I'm struggling for some synthesis around three distinctions, and it's not clear yet what the relationship between them is, but one of those is a distinction made by Schneider when he talks about self-monitoring. He finds that some people are high self-monitors. These are the people that are constantly regulating their behaviour from situation to situation. They're into Impression Management. Then there's people who are low self-monitors, who don't monitor their behaviour and they're more into self-exposure. And this turns out to be a matter of the philosophical position as to the nature of identity.

The people that are into Impression Management believe that identity is a function of the situation and one should be flexible and adjust one's identity to the various situations.

And this is very important. According to Goffman, the reason for dehumanization in total institutions is they take away your props, so you're not allowed that very human capacity to represent yourself as you want to represent yourself.

The second distinction is Rotter's concept of Locus of Control. Some people have an inner locus of control and other people have an outer locus of control. And it seems quite consistent in the research that people with an inner locus of control are people who are confident in the world. They believe that they are responsible for their behaviour, their freedom of action, whereas people with an outer locus of control believe that their behaviour is determined by some force other than themselves.

I'm arguing that whether you're a high self-monitor or a low self-monitor, it doesn't matter-that's a matter of philosophical position, but it does matter that you have a concept of inner control. In other words, you yourself choose to monitor yourself in certain situations, disclose yourself to certain people, and to monitor impressions to certain other people.

The distinction between intimate contractual relationships, I think, provides us with a useful basis for deciding in what situations we'll disclose ourselves and in what situations we'll manage our impressions. The distinction is that in contractual relationships, people are interchangeable. When you go to your grocer, it really doesn't matter to the grocer that this particular individual pays money for the groceries, and it doesn't matter to you as a person that this particular grocer stocks and sells those goods. However, when you take those goods home and cook them for your mate, it is important that it is that particular mate you're cooking this for and it's important to her or him that it's you that's doing the cooking. So people aren't interchangeable in intimate relationships and it would seem that in intimate relationships we want to make an open and honest presentation of ourselves, but in contractual relationships, we want to manage our impressions appropriately. In the original paper, I said in a perfect world, we would all be into self-disclosure. But I don't believe that any more. I believe we can handle only so much intimacy. If only for the fact that we've only so much time, and I believe that relationships are intrinsically intimate. I believe a stranger is just a friend we haven't met yet. But I think, with most people, we have an understanding that we won't realize the potential intimacy; that the fellow who sells a newspaper on the corner - we just have this tacit understanding that you give me a paper, I'll give you money. We're members of the same planet, and in more or less the same predicament, with essentially the same equipment.

I'm trying to use these three distinctions as a basis for developing a synthesis between the self-disclosure position of Gerard and the Impression Management position of Goffman. So extrapolations - these are pretty well as is in here; first of all the extrapolation from the present personal databanks which are scattered here and there in various insurance companies and credit card companies and so on, to a national databank; and this I describe as a bureaucrat's dream and a humanist's nightmare and I just realized, when I was listening to Neil that the bureaucrat who would like to issue the S.I.N. number at birth is introducing a whole new concept of original S.I.N.

For the extrapolations, what I'm trying to do here is suggest that the certain situations some of us find ourselves in and those personal databanks, as they get more sophisticated, may possibly put us all in those situations. The first situation is some of us are prejudged. That is, on the basis of colour of our skin, or that we have a female body, people prejudge us and there's a lot of evidence of the debilitating effect that has on us. Someone before they meet you can go to a personal databank loaded with information about you then essentially they are able to prejudge you and this limits your capacity to manage your image.

Some of us are famous and we all know about the identity problems that famous people have. They are prejudged as a kind of personal prejudice or judged on basis of their image built up by the media. Most famous people accept that as one of the unfortunate effects of fame but if indeed people can get information about us from personal databanks, we all become famous without any of the compensation. I believe I told a story, I don't remember if I told the story here, about a friend that came into the office and I wanted to impress her with my new toy so I said, "Let's see what my friend the computer in Santa Monica, California knows about you ..... " Anyway, I pumped out all sorts of information about her and she was flabbergasted, and I said, "Well, read it. Don't you know that that is available?" She said, "Yes, I knew it was available, but I didn't know it was accessible." It shook her up that within thirty seconds I could get a lot of information about her and so could a lot of other people.

Some of us have police records and we all know about the problem of how it becomes very difficult to re-enter society and how easy it is to slip back into the community where you are accepted, namely the criminal community. If personal databanks tell about us then we all have records and this produces a certain kind of problem in everyday life, namely because there's a record of your past you are more tied to that past, we become victims of our past. To know that we are beginning to struggle clear of the Freudian influence, we begin to recognize that the past is a useful explanation but a lousy excuse. But as more and more information is available about our past we tend to get tied to that past and we are afraid to live our life as an experiment because there is a record made of it. We have to find ways to build in forgiveness.

Some of us live in total institutions. As I said before, the problem with a total institution is that your props are taken away from you, making you unable to present yourself the way you want. These databanks take away your props, in effect. Those of you that come from villages know the difficulty of living when your life is constantly monitored by the neighbours. I found that life in a village was hard when I came here, - there's nowhere to go. We in a sense then all live in total institutions if indeed this national databank involves a lot of information about us and it is accessible to a lot of people.

I put some implications here in terms of the public, implications because in a more philosophical, theoretical concept the information society was shifting from a level of energy systems to a level of information systems, recognizing that there is a substrata of energy which is processed information. I think it is necessary to control systems, recognizing that there is a substrata of information which is necessary to maintain control. With respect to the individual, there is inner control and there is outer control.

Now let me start with inner control. Namely personal freedom. Then there is a matter of outer control and that is between the power of the person and the power of society in a democracy. And if there is no inner control nor outer control then we are out of control and that is where you get into the people in our prisons and mental hospitals who are out of control and cannot function.

The discussion resulting from this presentation focused on the need to clearly differentiate between individual autonomy or action versus autonomy of the group.

Other issues considered the role of the machine either as facilitator or as a modifier. The machine (Videotex) is viewed as a modifier of how information is handled and as a modifier of behaviour. The concern was expressed that the technology changes individual expectations about privacy and alters the concept of what consititutes autonomous action. This is particularly the case as these machines become integrated into a life style and dependency is developed.

A concern was also expressed about the structure of Videotex systems and their impact on privacy and autonomy. The question was raised about whether there will be a choice in providing decentralized systems where anybody can create their own data base and be able to plug into a network. The control of data bases and the gate-keeping of Videotex access by corporate or government interests was viewed as limiting the freedom of individuals to create data bases. As well, Videotex was viewed as a facilitator for the integration of data bases.

Concern was expressed that the choice of structures would be limited if large corporate interests dictated the system configurations. Thus, a critical component in helping to protect rights, personal autonomy and privacy is structure. There was an expressed need to encourage the development of alternative structures in the provision of Videotex services.

The key points arising from the first stage in the discussions included:

a. The need to consider the moral issues related to privacy. The concern for human freedoms and the right of individuals to choose.

   The right to choose includes providing information and participating in a particular system.

   The need to limit the use of information for purposes other than those directly related to a given or stated purpose. The need for an individual's data files to have a limited lifespan and to be open to personal inspection and scrutiny.

b. In the socio-psychological context, the key issues include the need to consider the loss of autonomy and security when addressing the issue of privacy.

   The concern for autonomy emphasises a fundamental feature of human behaviour. Thus the effect of new innovations, such as

Videotex, can be viewed as influencing some very basic psychological needs.

The underlying aspect of autonomy is the ability to control one's life. That ability, it is argued, depends on the individual's psychological make-up. However, systems such as Videotex can be used in ways which prevent individuals from directing and controlling their own lives. Whether perceived or real, such a threat represents a potential impact on the individual. Consideration of the effect on autonomy underscores the need to develop mechanisms and procedures of operating Videotex systems such that users can maintain a sense of security and not feel threatened.

2. GATHERING PRIVATE INFORMATION

The second major area of discussion was directed toward gathering of private information. The first presentation dealt with the concept of information as a commodity and the threat of Videotex systems to intellectual freedom. The second presentation focused on the alternative structures for providing Videotex and the impact on gathering information.

LOIS BEWLEY

PRIVACY AND THE INDIVIDUAL

GATHERING PRIVATE INFORMATION

As a former librarian, and now a teacher of qualified librarians, there are two major concerns we have regarding Videotex or Viewdata or Teledon or Prestel or whatever name you want to call this structure, and that is that technological developments have caused and will increasingly cause information to be a commodity--something that can be bought and sold. The second is that data retrieval systems pose a greater threat to intellectual freedom and control of intellectual property than I think has been faced. The rapid mechanization of information handling and idea dissemination does provide an invasion of personal privacy. What is there may be limited, so it's a negativism almost by withdrawal or a denial of access.

And to return to the question of commodities, I have absolutely no answers, but there are some questions that I think are well worth asking. Who determines what's available in a public as opposed to a private data base - David's think tank? Will only commercially viable information be programmed? And if so, who chooses it and from what sources and at what charge and through what mechanism? And how complete will the information be in any programs? Suppose you're looking at acid rain. Will any data file or data base on acid rain have company and corporation information? Will there be newspaper reporting in the file? Will there be chemical, environmental, ecological reports in the

file? Will government and private opinion statements be selected and put in the file in some way? Will the history of concern over acid rain or the effects of acid rain be in the file, for what--one week, one month, one year, five years, ten years, fifty years? What are we looking at? And who, in essence, will control the data bases and access to them once they are created?

And another question which hasn't come up here, but I think is related--what other kinds of non-electronic interference with access to these data bases will exist? And can that be viewed as some kind of denial of autonomy or again, by denial of access to information, is this in some way affecting our privacy as citizens? You know, producers of electronic program software and access to it, I think, will have to become as aware as the traditional publishing forms in print and other media, in that they are looking towards a market with an identifiable needs slant. Information need for all of us, in one sense, is an infinite thing, when we look at all of it. But for individuals, there are specific information needs we have. The traditional publishers have focused upon those needs to make their profits. Is this going to happen in electronics information processing, or will there just be something that is potentially very lucrative handled by some kind of conglomerate structure? I don't know. I do think to have an informed, alert and literate citizenry, access to a variety of information and a variety of forms of information are certainly necessary.

More specifically, I think Canadian librarians and information scientists, as all Canadians, should be very vitally alive to the threat of the control over Canadian content and of Canadian information in commercial data bases. Librarians are looking for representation on Vispac and I know they're trying to be represented on the Canadian Videotex consultative committees. Looking at such things as education and the social implication of the new technologies, I think, on the technical side, librarians can help to modify the rather cumbersome tree-structure searching methods that are available on the current Videotex systems. I suppose, in essence, my main concern is whether accommodation to the electronic data processing modes will so manipulate and manage information that it will be truncated and abbreviated, or proscribed, so that it can be packaged for sale. Now this is a very traditionalist, very humanist point of view,

which I think reflects a good many concerns. I am not denying, and I'd be a fool to do it, that this kind of access to information is just a God-send.

DAVID GODFREY

PRIVACY AND THE INDIVIDUAL

GATHERING PRIVATE INFORMATION

I think we must bear this in mind: three types of levels of systems are going to exist at the same time whether we like it or not. In a sense the only one that might not make it is what I call "Secret Super CPU". This is the national level total data base where you find out where your Aunt Sally was born. Now this, you know, might happen and there might be certain kinds of information that one wants to put into that but I think there's a scale up here, a scale of neutrality of information. Godfrey's law is that the more information that is gathered in one place, the more neutral that information ought to be. The other level which will be briefly called "network notion" I tend to favour. To get some of the advantages - where the nation state or the larger social group would in essence design a set of common protocols and have a sort of "think tank" of people designing data base software and then giving it out and putting it out in the public domain. So that in this type of system, you know, I keep using Greenpeace, but let's say you have Greenpeace on this end and U. Vic on this end and University of Manitoba, whatever, here, okay, so you have these individual groups building their locally related data bases of information and yet doing that, not on the same system necessarily because these are sort of temporary lines that could always go this way, but with enough commonality of software communication links in all the sub-sets so that they could transfer information if they wanted to. That's what I call the network model and that would come for sure. The hub is in this model a "think tank" that provides standards. These aren't really communication links. To a certain extent, it also might, might provide some kind of satellite channel or it might be the electronic roadway.

It's not necessarily a carrier, because all these networks are not networks. They're not permanent networks, they're just sort of temporary links. It's like thinking of everybody on the telephone: there are an inevitable web of networks at any given time when "A" is phoning "B" and "B" is phoning "C" if they are all connected. So these are just possible configurations within these networks but there are going to be social groups that develop information stored on computers which they want to exchange with one another.

Well, it becomes impossible to draw these diagrams because they get so large, I'm just trying to keep them very simple. In theory, this could be let's say, this is the Vancouver Public Library service to the network, and then this is Public School 39 with its group of students, let's say, who want to get some information from here, so they might have to go through this node which is not necessarily a hub, in the center of the network.

U. Vic may be an external hub, providing the kinds of service that the individual needs or you may have a little network of Apples out here. The network is the sort of total open model. You may have a network of Apples in Victoria, right, and they may decide that they want to get over to this Greenpeace Halifax system and there may be some way for them to have to get through it. It may go through U. Vic and provide the services, there's not necessarily one hub, there's levels of hubs.

The network has no personality in itself, except to the extent that it's opposed to this model, I mean, somebody was saying from Manitoba Tel that someone phoned up from Chicago and wanted to get their information on airline reservations out to the IDA trial in Manitoba but didn't want to do it through ..... Infomart. This model lets you do it. This model in a sense doesn't let you do it because whoever is up here on these key control points is going to control, in a sense, the information that comes in. Now, there are however, in a sense, still lots of problems because one of this group may be the Victoria Rape Centre. Now, I don't know if we want to keep taking this as our example, but let's say, Dave Godfrey as rapist is in this databank? Now in this system, obviously, he's not going to get into the system, because there's going to be a

monitor who says, "I'm sorry you can't call someone a rapist". This one in a sense does because there's DG as rapist, and all of a sudden there's DG as rapist in Halifax.

The third model in a sense is the private anarchy thing, where nine people get together? Nine people get together and set up their own network of whatever kind of information they want, which could be radical or could be social or whatever. People buy little $400 terminals to plug in. So, for the private anarchy model, technology is available for it right now, with very restrictive access.

When I looked at this I said; What are the traditional issues in terms of information and information of value? What is the threat? How do we look at protecting it and what new issues are coming up? So, it turned out that most of these things could be looked on as something that we possess which can be threatened and which there are certain laws to protect and I leave this to the lawyer's department. But there's your good name, okay, in which there are threats of slander, libel and in a sense, old truths, and there are protections, libel law and human right legislation. There is intellectual property which is your copyright in the book that you write and the threat is that there is cash for goods and the threat in a sense is misrepresentation. You get information which is false and therefore you lose some cash. Protection is provided by consumer rights or whatever in society. There's the possession of knowledge and the threat is denying access and that's where the printing press, in a sense, was phenomenally useful in changing society because it stopped starting denials of access to information.

Then there is individuality and what I call, groupology - one has to almost deal with them together. And again the threat is intrusion and then alienation and ultimately dispossesion. In other words, when my grandmother went to work on an Indian Reserve in Saskatchewan, ultimately she helped destroy that group. She also saved their lives by saving them from smallpox but, you know, then there are threats to groupality. Okay. At the larger level, in a sense that information can be looked at in terms of what is the nature of the group. There,

in terms of the preservation of the nation, the threat is the destruction of habits of the group.

And then the final thing that I will leave you with is the new terms. ..... LRP, LLP. This is what I call, the life line pattern, the life medical pattern, the life trained pattern, the life travel pattern, life burning pattern. That, I think, to me is dangerous that you will start being able to gather this kind of a profile on people.

The discussion of system structure indicated that a variety of architectures are possible for the provision of service. It was considered important to accept that there are a variety of models which should be encouraged. Such developments were considered important in avoiding the accumulation of data bases and controlling of information by only a few system operators and information providers.

A critical concern was the need to allow wide representation of information on Videotex systems and to allow access to information from a broad base of users. Such broad based usage was thought to discourage the manipulation of information and system operation by a few large organizations.

An important phase in the development of Videotex was the stage of two-way interaction. At that stage, sub-networks of private interest groups could be encouraged to develop and to generate information and exchange ideas.

Analogies were drawn between the developments of a broad based Videotex system and the development of the printing press. The freedom of expression and the fostering of an open system were considered positive developments to limiting the loss of personal autonomy and privacy.

In those instances where data bases are stored in one central location, access can be easily limited. However, the opinion was expressed that

perhaps such data bases should operate - much as libraries do - on the basis of public access. Data bases may be viewed, in many instances, as public goods where access should be available equitably. Fostering equitable access would be possible with a broad based decentralized networking structure for Videotex systems.

The marketing of information as a commodity was viewed as a factor which encourages the filtering of information. Information which is saleable becomes manifest on the Videotex system, while that which is not saleable or is potentially damaging to the IP's marketability is suppressed. It was considered imperative to encourage the development of community or public data bases as compliments to commercial information.

The notion of information as a commodity was discussed in terms of its unique qualities. Information was viewed as being different from a physical commodity since the vendor still retains possession of the original information. That aspect was considered vital in assessing the impact of such systems on copyrights and ownership of information. The rights to information need to be defined and the need also exists to develop legislation which deals with these new technologies and the issue of copyright.

3. PROCESSING AND STORING PRIVATE INFORMATION

The initial discussion in the third part of the workshop dealt with the way data processing systems are organized and the problems of data storage. A critical issue included the loss of control when large centralized systems are developed. The situation can develop where there are large programs and nobody quite understands their operational feature. In such situations, control is lost and the user is at the mercy of the system. In many cases, the programs are dealing with personal information.

A second issue identified the danger that standards of quality and security may be used to restrict the development of smaller, more decentralized systems for providing Videotex services.

DOUG SEELEY

PRIVACY AND THE INDIVIDUAL

PRIVACY AND STORING INFORMATION

When you look at Videotex and the realm of ideas, we're examining in our discussions a number of alternative kinds of information exchange systems. Where there might well be information exchange systems which deal with buying and selling bits of information, there also could be systems that can run into work.

This kind of a system John and myself experimented with was called Community Memory. Essentially it was really an educational bulletin board, in which people were free to enter information and to exchange information in an almost totally uncontrolled fashion. We saw that, since it was an experimental situation, we didn't really see its total use, we only could see a partial use of it.

I think there should be room for these kinds of networks. Videotex could be a medium for such activities, if you look at sub networks.

I believe my reading of the law at this point says that you only need to give the S.I.N. to the tax people and to the census. There's a very narrowly defined area by law that you need to give S.I.N. to.

And your passport.

Any federal department which requests it.

But there's another interpretation that is not that broad. It certainly doesn't go over into private use. The reason there should be no S.I.N. is because with the new kinds of networking possible, information collected about you from a number of sources can be integrated much more easily than it could ever have been done by hand. So it isn't just a change in scale, it's a change in quality, because some things are now feasible that wouldn't have been considered before. So with Videotex or with these computer communications networks, there is a quality of change. This isn't really related--just sounded a bit religious as well.

In the Jewish culture, a long time ago, every seven years, all debts were forgiven.

Data that dies might be another part of this, but I'd like to focus on programs. And the point..... is that large-scale programs such as accounts receivable programs at B.C. Hydro, tend to grow for a period of years. This occurs through the group effort of a team of programmers who are in continual transition.

The rationale behind the way in which the different module of these programs are put together gradually becomes more a matter of mystique than of direct knowledge. No one really knows just how so-and-so programmed that sub module to double-check on your S.I.N. Over a period of time, this gets worse and worse, so I believe - this is a point that I heard originally put out by Weisenbaum - over a period of time, programs should be written off, and the money that originally went into them should be put into the development of new programs. Otherwise, you will have situations where there are very large programs--nobody quite understands how they work, and hence we have the delegation of your

responsibility to those programs. That is important because many of those programs are dealing with personal information. Here's a hypothetical consideration: right now France, England, Canada and Japan are looking at the top down implementation of large-scale Videotex systems, along with large corporate interests and in Canada, we have a bias towards those kinds of interests because we need to compete with the giant sitting next door to us. Well, what I'm afraid of is that people will take a look at the hobbyists, the personal computer people, and small-scale business operations that are now in communication with the computer networking, and say look, there is no insurance on the quality of information you're exchanging. And, as well, that there is no way we can keep those people who have their terminals from getting into private information, and doing what they want with it. There is a great deal of computer crime going on, and I can see a scenario where vested interests would say, look, we can't have all those little anarchists running around with this potential for all that computer crime and all that invasion of privacy. So we have to restrict the way in which information gets exchanged, and it has to be channelled to go through gatekeepers.

What I'm suggesting is a possibility here. As much as I believe in privacy of personal information, I can see where it could be used to limit freedom of expression over computer networks and consequently to limit the creation of culture.

For instance, in B.C., Dominion Directories and B.C. Tel have a common owner and that common owner is an American Corporation. That corporation owns a major telecommunications carrier in the States. Now, we've got that kind of vertical integration as a component that goes into this industry. I think there is reason to at least ask the questions to be sure that there isn't a restriction of free competition. So, we may have to have some mechanism for ensuring that that is not happening.

I'd like to see as little regulation and control in these networks as possible. I'm sure that some will prove to be necessary and there are concerns about these areas being met. Also, I would like to point out the notion of pre-emption. As I

was saying earlier, the kind of research we have been doing at Simon Fraser and the ownership and distribution of data bases suggest that this field is being locked up in a hurry. In a sense, the marketplace is going to be pre-empted. There is actually not going to be very much competition. By the time these things become on-line, they're brought about by interests which will make competition very, very difficult.

The second area of discussion dealt with issues of billing and the role of information providers to secure the records of users. Billing under a centralized Videotex scenario would most likely be on a user-sensitive approach. Thus, records of usage, tracking of consumption and page selection could be monitored. That situation leads to the possibility of cross-referencing of files and ultimately to the linkage of Videotex usage to other data files using common indentifiers, such as a Social Insurance Number.

REX SCHOFIELD

PRIVACY AND THE INDIVIDUAL

PROCESSING AND STORING PRIVATE INFORMATION

It is frequently said that we are entering a new era, the information age. Mankind has bought and sold information for profit for many years. What we are doing is entering that era where the distribution of massive amounts of information has become relatively easy and inexpensive due to technological advances and therein lies some major problems for privacy.

Examples of information gathering and selling from past markets could be such things as espionage, the careful and sometimes dangerous game of gathering information of varying amounts of value either for an organization or for sale to the highest bidder. Lawyers who pay clerks, articling students or junior lawyers to research and collect precedents for cases. Companies who have whole research arms for data collection. In fact most companies run on "information"

which they choose to call statistics, sales results, budgets, contracts, etc. All of this information is valuable to other than the original owner. But let's look at a more basic type of information gathering and usage. As we commence field trials in various areas of Canada, one area that is far from resolved is billing. Once Teledon becomes a public offering, how it is billed could have a serious impact on privacy, both personal and corporate. It seems generally that the thinking regarding how to bill for Teledon is based on the user-sensitive approach; that is, the user will generally pay according to usage, so much per specific page of information access. Perhaps connect time charge for computer utilization where interactive facilities and time are a factor. That ensures that those who use the system the most, pay for their use and they're not subsidized by others. Commendable, but such a procedure will require a detailed record-keeping in order to bill and collect revenues. Now we can begin to draw a detailed picture of your interests and activities. Look at it this way. You probably receive a daily paper with a broad range of information, from world news to local gossip, sports information, business news, investment and market reports. You read what interests you and no one knows what that is but you. But if you have to call all that data up and pay for the time, pay for just what you use, now the information providers also know what you read or utilize the terminal for. Gather together all the data from all the information providers, and we can draw a detailed interest activity profile of any individual or company. Truly "1984"--and potentially in intimate detail. Even if it turns out that billing becomes a flat rate approach, information providers will need to track usage to see what pages are used and what pages should be discarded, and they will never pass up the opportunity to draw a segmented profile to show what this or that ethnic group, income group or any other identifiable group needs, looks at, uses, or otherwise has cause to access any specific page, group of pages, specific data base or type of information. That would be a temptation beyond the strength of any marketing person. There's been a great deal of concern generally about the use of S.I.N. which has been discussed a few times today. It provides a convenient scapegoat for "1984 style scenarios" wherein all manner of data is collected and sorted against someone's specific number. But in the modern world of technology, it is easy to interface various files, created on

different keys and come up with a master file of integrated records by person. The S.I.N. is a symptom, not a disease.

What is of concern is the relative ease with which data about individuals or corporations can now be gathered and stored. And where do you draw the line? In respect to corporations, where is the fine line between the competition analysis used to evaluate competition in the marketplace and an excessive amount of information used to deny or destroy competition? At what point does information about an individual pass beyond the needs of marketing to that particular person's specific requirements or interests and pass into the realm of control of that individual's life? All tempting data to collect, much of it innocent in the extreme, when not assembled correlated and analyzed. Whether used for covert or for overt action, such data would be economically valuable in the extreme. Another factor is the temptation to its being gathered, processed or sold.

It would be quite possible to enact legislation requirements to destroy individual records after billing or even after a specified time period. You could negate their use under penalty of law. One would assume that such legislation would permit the folding of such information into generalized statistics, rather than a record of an individual or corporation, since from a practical business point of view it would require fairly detailed and specific records of page access information in order to make the decisions necessary to success in the world of the information providers.

In a more general sense, the whole question of processing and storing private information in both private and public data banks must give rise to severe concerns. We have recently been exposed to various news stories of computer crimes, where unauthorized access has been obtained to data banks, either for profit or for a prank. The concern has to be not why, but how? If we are to store widespread and detailed information about associations, businesses, governments, organizations and people, then unauthorized access must be a major concern. Consider for a moment your personal income tax return being available to your perennially nosey neighbour. Credit rating and spending habits,

there to be checked out before you accept the date from the blonde Adonis in the office. An infinitely detailed record of every piece of information you have looked at in the last five years, available to anyone. The list is endless. And not just access. What if someone could get in there to change your credit rating or give you a criminal record? Some increased degree of security will be required in this new world or it will not be accepted by the masses and without large volumes. Videotex will have little appeal to those who have to put up the capital to get it off the ground.

Speaking of criminal records, the Canadian Association of Chiefs of Police presented a brief to the Commons Justice Committee which was studying the proposed Freedom of Information Bill and the related amendments to the Privacy Act. In their brief, the Association said, and I quote, "The truly innocent have nothing to fear from Police access to personal files." Perhaps, but I tend to support the attitude of everyone I know who takes the approach that my personal file is just that--personal. To allow unlimited access to personal files by police or government to simplify their jobs--but most of us are not yet reconciled to living in a police state. Necessary legislation to protect the innocent from unwarranted access to their personal files or histories may well protect some who are not so innocent. It has been thus for years in a free society and the information industry had best remember that!

But enough of that. As a businessman, I find the prospect of Videotex services as exciting and fraught with opportunity. From a positive standpoint, it can enhance our knowledge, provide a communication medium that could bridge the gap between races through multiple data banks or through automated translation services, make large funds of information available to those who, by distance or infirmity are now largely denied that ready access, provide jobs in the high technology area for Canadians and, without question, change the very way in which we and the rest of the world think and live.

In today's world of over-regulation, one hesitates to recommend more. However, regulation in itself is not a bad thing. It is what and how we choose to regulate that determines good and bad legislation. From the perspective of the

businessman, we would hope that the government would choose to pass laws that protect the essence and substance of privacy, without feeling that they must list in great detail every step required to achieve that goal. To borrow from Doug Parkhill in "Gutenberg II", stringent legal safeguards will be required. These could include:

1. Creation of a corps of bonded professional computer operators bound by a strict oath of secrecy.

2. A total ban on disclosure of personal information from the files, except for the individual named.

3. Mandatory security measures, both physical and electronic.

4. Severe criminal penalties, including mandatory jail sentences, for breaches of privacy on the part of the "keepers of the files", and for those police, government and company officials, etc., who incite, condone or benefit from such breaches.

5. Civil redress for those who may have been damaged by improper disclosure of the contents of their files.

6. Mandatory destruction of certain types of information might also be required so that certain types of master files cannot be created.

Mr. Parkhill goes on to say that individuals should have both access to and right of change or destruction to any files held by an organization. Presumably, he did not include the government as an organization so constrained!

Perhaps I might make some comments from my perspective. I am not sure that bonded corps of operators is really a necessity. Those that we have now handle a great deal of sensitive and confidential material without serious problem. Certainly the creation of severe criminal penalties as suggested in Item 4 would seem to be an adequate alternative. I would agree totally with Item 2 on a total

disclosure ban. I think that even without Videotex that is an area that has never been properly addressed. I feel much the same about Item 3, mandatory security measures. I think that measures to provide security for physical and electronic data is absolutely essential if we are going to get into this area. We need to have legislation to provide for the need to provide data and to protect adequate penalties if we do not, but the details of how can quite likely be addressed on a local basis. Item 5, for Civil Redress, again needs to be covered with or without Videotex. As indicated earlier, for records and details of a specific individual, organization, company, etc., access to particular pages of information should be maintained only as long as required to provide for billing and collection functions. Release of this information to other than the individual concerned should be punishable by strict legislation. Once those functions have been satisfied all such tracking information should be purified to remove permanently any reference to a specific group or individual. In addition to this, it might be wise to prohibit the creation or possession of any "master" file or data relating to the activities of a specific individual or group. The recent privacy act seems to have largely resolved the question of access to files on one's self and one would assume that the same provisions would apply in the field of electronic media.

To summarize, the tendency to accumulate data for marketing studies, for sales leads, for curiosity, for whatever, will be great. The consequences could be disastrous whether that collection is private or government, innocent or evil! Security to prevent unauthorized access to files, either to examine or to change is more necessary than at present and must be as near to fail-safe as possible. Videotex has the potential to truly change our world. Let's make sure it's for our betterment!

A key issue raised in the discussion of these presentations questioned the limitation of freedom attributable to corporations. It was argued that, in fact, it is more likely there would be limitations as a result of government legislation. The development of laws could have a more restricting influence than a particular corporate action, which tends to be self-serving but somewhat limited in scope. Competition in the market place will, it

was argued, prevent the domination of the industry by one sole supplier having the ultimate power to control data collection and acquisition.

As in other areas of discussion, the need to avoid only centralized system development of Videotex was viewed as necessary to protect the privacy of individuals.

In addition to system networking, a key concern was the need to encourage a broad range of information providers. Through that development, the ability to limit the control of data by any one group is encouraged. Once again, the two items of interest were: avoiding the super-central storage of information and the need to encourage maximum flexibility for accessing and using data.

4. DISSEMINATING PRIVATE INFORMATION

The final section of the workshop dealt with the dissemination of private information. This focused on three areas: the legal remedies, secondary and tertiary use of data and the role of citizen advocates in protecting individual rights.

The discussion of legal remedies addressed the issue of existing legislation relating to copyright, contract law, libel, slander and common law. In addition, attention was given to existing legislation specifically related to protection of privacy on a provincial and federal level.

JACKIE KELLY

PRIVACY AND THE INDIVIDUAL

DISSEMINATING PRIVATE INFORMATION

I thought it might be worthwhile if we spent a few minutes discussing some of the legal protections that are available to the individuals in the context of information. A number of people have mentioned copyright protection. That, I think, has limited utility in that it protects the expression of ideas, not the ideas themselves, so it doesn't offer much protection of information for the individual.

There are a number of other legal remedies in a contractual setting: we have a remedy of breach of contract, one of the prime examples being the doctor/patient relationship, which is a confidential relationship. If the doctor discloses information, i.e., discloses information not permitted to be disclosed, you would have cause of action against the doctor. The first thing you must know is what the doctor has disclosed; secondly, in the context of breach of contract, you've got to prove damages, so you would have to establish what damages you suffered and can recover against the doctor.

I think in most instances there are written contracts. What occurred recently is a Royal Commission ppointed in Ontario to investigate confidentiality of medical records. I think you really are importing an implied term into an unwritten contract and there is some support of that in various establishments that require some kinds of information be kept confidential, things like medical records, you are really stretching to get to the point where you say, that in fact, I go to the doctor and that creates a contractual relationship.

Intent isn't really relevant in the context of the breach of contract, though it's relevant in the context of some other legal remedies that you might have - breach of confidence, for example, or breach of privacy. Breach of privacy is an action, where intent becomes relevant to the quantity of damages, but basically on a contractional basis the whole object of the law is to put you back in the place you would have been in had the breach of contract not occurred. The breach is an implied term of non-disclosure. If you can show you have suffered damage because of the disclosure, quantify that and intent.

Well, you can sue someone for wrongly disclosing information. It's really a question of how far the courts will go in assessing damages from that kind of situation, because there is a third party involved, ... and there you get into a non-contractual kinds of remedies.

Remedies for breach of confidence, breach of privacy, are not really well developed actions.

Non-contractual relationships; that is, not having a one-on-one relationship, are probably more relevant in the context of what we've been talking about. That is, people disseminating information who may not necessarily be people to whom you have disclosed the information. You really have to look not in contract but in libel and slander. Basically, incorrect information is disseminated about you and you suffer damages so you have the right of action against the person who is disseminating. That helps only as long as the information is incorrect. The truth is a defense to an action of either libel or slander, so if someone is disseminating true facts about you, libel or slander isn't going to help you.

Also, there are limitations on libel and slander actions in that the defense qualifies privileges available. That is basically, "I said what I said without malice and because of a higher duty I had, somebody had a need to know." An example, I think, given in the royal commission report was what happens if you have a contagious disease: you've got VD, does the public have the right to know? Not the public generally, but do medical authorities have the right to know who has VD or other contagious diseases? So that's where the defense of qualified privilege can arise.

Another kind of action is an action for breach of confidence, which is really an old kind of action but not tremendously well developed. It is an inequitable action. Normally in equity there is no right to damages. If somebody breaches a confidence, you can get an equitable remedy including an injunction to stop people doing that in the future but not necessarily in actual damages. As far as I can determine, that action, as I say, is not really well developed in Canada and it's really impossible to say what real rights, if any, an individual has in this kind of context.

Another kind, also inequitable, is common law action. For breach of privacy and this really brings up something that Rex mentioned, there should be legislation protecting individuals, protecting their privacy to the fullest extent. In fact, we have legislation like that right now. British Columbia has a privacy act which says that you don't have to prove damages to be able to sue. If somebody has wilfully violated your privacy, you can sue them. We had that legislation here since 1968. To my knowlege nobody has used the act and basically in Canada actions for breaches of privacy are very few and far between. So I guess that points out one of the problems of having general legislation which doesn't define what is meant by the breach of privacy.

Four or five of the provinces have privacy legislation and I think almost all of them have come up with some examples that deal with specific situations, using somebody's name or their picture. I can't recall what some of those other provinces are. One of the provinces, I think it may be Manitoba, actually has a list of remedies, others are trying to prove that your privacy has been violated.

Certain things are defined, but B.C. doesn't have that. So basically you're back into the courts and the courts will determine what's reasonable given the circumstances. The B.C. act also says that the nature of the degree of privacy to which a person is entitled is that which is reasonable in the circumstances, which really isn't that much.

The other kinds of exceptions are, of course, the usual exceptions for police officers ..... in the course of their duty or an individual authorized or required under the law in force.

One of the problems with the common law action for breach of privacy is that there has to be public disclosure and there's some indication that disclosure to a limited number of people or members of a group may not be public disclosure.

If you publish to one person, that constitutes publication. Again, this is not an action that is well developed in the sense that there are a lot of cases in Canada. There is also some indication that disclosure would have to be of a nature that under the circumstances would be offensive to the reasonable man. You are not saying, I guess, that what was disclosed was important to me as an individual but that what was disclosed had to have been important to the reasonable man.

Well, it is all very vague. I guess that is one of the reasons I raised it. Yes it is vague and there aren't a lot of cases, but the remedy does exist and I'm not sure that you're going to get much further by having the same kind of legislation. You may have to get more specific or you may just have to have more people complaining and using the existing remedies in an attempt to build up some precedent.

There is privacy legislation in the federal context in the Canada Human Rights Act, but it only really relates to information like let's say, federal information banks, and basically you have the right to get access to that information to ascertain what uses that information has been put to, to request corrections if you feel there are errors and to require a notation if they refuse to make corrections.

The key results from the discussion of legislation focused on the difficulty of defining the term "privacy". Where legislation does exist, it seems to be rather broad and open to a variety of interpretations. Thus, bringing action within that legislation becomes increasingly difficult. Actions which have been made generally required a specific context for judgement and were considered not in relation to a specific individual but rather in the context of what was considered as reasonable behaviour.

The major difficulty with the current legislation relating to privacy stems from the diversity of areas which could deal with the issues. These include libel, slander, breach of contract and breach of confidence. Each of these terms proves difficult to define and require a clear definition of intent on the part of one individual to prove guilt. In many instances, the magnitude of damage caused by the action is difficult to quantify and, as a result, assessing damage becomes quite impossible.

In the legislation area, there exists one set of laws dealing with the issues of data communications and activities, such as data transmission and collection. These generally are federal laws dealing with trans-provincial data usage. When dealing with privacy, the actions must be dealt with in terms of a particular event, such as libel, slander or defamation. The need exists, therefore, for legislation which limits the access to individual data records thereby facilitating actions which violate individual rights of privacy. Such legislation, on the federal level, exists in the form of the Canadian Human Rights Act. That relates to information stored in federal information banks. Individuals have the right to get access to such information in order to ascertain the uses such information has been put to and to request corrections, if there are errors.

Critical problems identified with legislation on privacy and data banks includes the policing and relevance of such legislation in a rapidly changing technological environment.

The second area dealt with in the final section of the workshop focused on the secondary and tertiary use of data. Such data would include customer profiles, user tracking data and information usage. The assumption was made that such files are likely to occur in Videotex operations where centralized networking is provided and large information providers are operating. The issues investigated included the methods already in place to help guarantee personal autonomy, the use of identifier codes with limited access and lifespan and the problem of tertiary uses of data. Tertiary uses were defined as those beyond the profiling activities and might include the selling of customer lists to a third party.

PETER BOOTH

PRIVACY AND THE INDIVIDUAL

DISSEMINATING PRIVATE INFORMATION

The particular issue I want to discuss is related to the operation of Videotex field trials that are either going on or will be going on in the very near future. The operation of those trials raises some interesting questions with respect to privacy. This is particularly the case in relation to the issue of secondary uses of data. In many of the field trials, we are immediately faced with the problem of secondary uses of data. That is, in the design of these trials, we have to deal with the system operator, the telephone company, we have to deal with the information provider, the large centralized information provider like Rex's organization, and we also have to deal with the user, and his reponse to certain operational characteristics of the systems.

What we are currently looking at with the field trials is one technological system, and that is a centralized system. Where we are at today is with the centralized operators and I don't necessarily believe that we are going to be in the same position tomorrow. I think, in fact, that this whole system is evolutionary and we are evolving into a more decentralized approach. But, the point is, I think, that the field trials can help evaluate, for example, not only the

response to Videotex operations and not only the response of individuals to the operations. The field trials also help to evaluate the degree to which a centralized operation of a Videotex system is useful to society, its utility in providing an equitable distribution of information that allows full and open access for individuals; the user, the IP, the individual IP's. I perceive the field trials to be just that and the evaluation of not just the user of the system itself, but the system architecture. However, there are certain characteristics of the trial that exist and I think that they have some relevance to the issue of privacy and the individual.

It's been a constant desire of most Videotex operators to get as many and as diverse a group of information providers onto the system. The user of the system will only evaluate it positively if he has information which is useful to him. It doesn't make much sense for Info mart, which has a whole database focused around central Ontario, to try and put that into New Brunswick and expect the users in Saint John to find the Toronto Community Information Centre has any relevance to them. As a result, they are encouraging the development of a diverse set of information providers. I think they also realize the need to encourage alternate structures in the set up of these systems. However, be that as it may, the current issue that comes up in the field trials is this: when you operate a system you are going to have information going into to peoples' homes, a select of group of people at this stage. What's happening then is that the choices that people make for information, whatever it is, can, are and will be collected in a centralized place. Profiles of individuals, their usage patterns, the time of usage, the number of usage sensitive variables can then be collected on these trial participants. So, in the operation of Videotex systems, two issues come up: cross-referencing of information, and the general secondary use of data. Now, cross-referencing of databases can be looked at in two ways: one is the cross-referencing of the Videotex files themselves and the second is the cross-referencing of the files resulting from the use of the Videotex system and such files would contain records related to user choices and characteristics. The collection of that information, at the present time, is in the hands of the system operator, not the IP. The IP has a vested interest in that information.

I don't think that the cross-referencing of actual Videotex databasing (that is, pages of information) is of critical importance to this discussion. I think the most important concern relative to the privacy issue is to the cross-referencing and access of these users' data files. Now, that issue has been raised as we design these trials. How are we going to protect the rights of an individual? If I wanted to, I could access an individual household and I could find out exactly what that household accessed and I know where it is and who it is. I could access that information, and I could get a full profile over a 12-month trial period of these individuals. I don't think that is terribly removed from what can happen, again, if we accept the existing system architecture in the actual system operation when we get out of the trial phase. The consideration of how you can profile an individual has been raised and the response to raising that issue has come from two areas; one from information providers and one from the Department of Communications, where last summer in July, at a similar meeting to this, terms of references were set up for operating trials. The Information Providers' Association, or VISPAC, has set out the issue, peripherally, I think, in its code of ethics. In their code of ethics they state quite clearly that where an information provider offers direct purchase of goods or services using the two way facility of the Videotex system, the user may be in no doubt as to the consequences of using that with respect to financial obligation or to voluntary disclosure of private information.

In another article, it is stated that no information provider will collect or cause to be collected any data or information about a user that is not necessary to the specific conduct of the information providers of Videotex or teletext operations. And no information provider will disseminate any such information or database such that a user may be identified or his privacy violated without express consent of the user. I think, though, that the important point is that in each of the articles outlined, the right of an individual to be aware of the uses of specific data is defined. In each case, the implication that there is an invasion of privacy is also made. What's happening in these kind of articles is the individual is given the knowledge that the information may be used in some manner. I think, fundamentally, however, the actual extent of use remains undefined. And in such situations, the choice of an individual is limited to not

using the system or not utilizing a particular service or system feature. So, what you've done is to restrict access. My only choice is to not use the system which again creates this exclusion barrier. I think that the important concern remains as the definition of the extent of secondary use or what I refer to as tertiary use of such information.

In another context, the Department of Communications has considered the issue of privacy in terms of secondary uses of data gathered in our field trials. Their response is to say that where you do have these tracking files and tracking secondary uses, each user of the system is protected. This is accomplished through the use of what they call an account identification number, and all data used for secondary analysis would be labelled with this account identification number. The same idea would be used for demographic and other data so researchers may relate questionnaire and usage data without knowing the identity of the source data. Researchers are allowed to use published data only when it has been aggregated over enough people so the individual cannot be identified. It is exactly the same procedure that the census uses, for example, when they go into an area where there is less than five people. Operators will make users aware that the usage will be monitored for research purposes. Each participant in the field trial will have to sign a contract. The DOC guidelines emphasize again the need for insuring the anonymity of the participants in the trial. The guidelines also suggest possible methods for limiting the use of information in actual Videotex operation. The prime importance lies in restricting the tracing of individual usage for purposes other than are necessary for the operation of the Videotex system. And in secondary and even tertiary uses of data, Videotex users, unfortunately in actual operation, would be totally unaware of the actual activity that has taken place. They have given information because they have said, if you want to link into this file, under the existing structure, you have to provide us with certain information and be willing to let that information go out and be used in some way. So, again, the important concern is the need to provide full disclosure. Such disclosure may, for example, be provided when the potential subscriber, if we assume it is going to develop into something like a cable system, is contracted for the service. It is then up to the provider of the service to protect individual rights

Now, the obvious question that arises is, how does the user know what is being done? Well, again, I think, technically, there can be certain safeguards that are maintained through the issuing of account numbers that you can't trace back.

I think that the important issues, then, are: the conditions under which we allow different types of information concerning the individual to be collected, the structures which can be developed to ensure equitable treatment of individual data, the constraints which can be placed on the storage and cross-referencing of the information, the limits which should be defined on the disclosure and uses of that information and the definition of rights of access. On that point, which I think Scott raised, the data that isn't in the system can be as important as the data that is in the system, in the sense that, when as a researcher you are dealing with large sets of data, you develop profiles and segments and you are assessing the response to the system and things become ideal. You are working in a quantitative mode and it's almost a normative kind of approach. There is no subjective evaluation of the individual.

An important point that was raised earlier was the issue of the use of information other than for the operation of the Videotex system itself. That is the secondary use above and beyond what is needed to operate the system and it is at that point that controls really need to be immediately recommended. The individual contracts to use the system, but doesn't necessarily contract to have this usage information subsequently sold or utilized in some way. The question on that point is back to restricting or maintaining the anonymity of the participant.

The discussion of these issues focused on the need to have control of user files and to limit the tracking or identification of any one individual using a particular system.

Other critical issues were the limitations of the use of data files for tertiary purposes and a full disclosure, by companies, that data about an individual may be used for some specific purpose.

The use of account codes with limited lifespan and limited connectivity potential, i.e., to build up macro data files, was considered a desireable step to limit the potential for invasion of privacy.

The final area of discussion dealing with disseminating of private information focused on the role of consumer advocacy groups. This dealt with specific examples of past experiences dealing with computer data banks. As well, the implications of new developments, such as Videotex were presented.

JEAN DOUGLAS

PRIVACY AND THE INDIVIDUAL

DISSEMINATING PRIVATE INFORMATION

I think probaby, the two main worries and concerns for consumers, generally, are privacy and access to the information. So we don't want to have one without the other and, of course, one of the basic consumer rights that we subscribe to is the right to be informed. I was going to mention the Federal Government privacy act, which is being revised, but that's been mentioned and covered, and the B.C. act has also been covered. In 1973, invasion of privacy was the theme of our annual meeting of the National Association and at that time we did some research across the country. That turned out some wonderful things such as our beloved company now known as Equafacts. At that time it was called the Retail Credit Company of Canada. It turned out to have some wonderful practices, including the fact that the investigators actually had a negative quota for insurance searches which was rather thrilling.

A great deal of personal information, which had nothing to do with the investigation of insurance came up: their political affilitations, whether they were known to gather with undesirables who were put into the category of blacks and other mixed nationalities and Asians, I think was one of the other wonderful definitions. We also found that the data that they were storing was already

outside of Canada in Atlanta, Georgia. We were there too late to have anything done to stop information about us going across international boundaries. However, as a result of that we became very upset about the credit reporting in general. I will not say we were solely responsible, but we were very instrumental, I'm quite certain, in bringing in what was at that time, in 1975, the Personal Information Reporting Act which is now called the Credit Reporting Act.

This man was approached by his firm and asked if he would like to become a Director of that firm and he said yes he would, it would be great, but were there any particular requirements? They said yes, we feel you should carry more insurance, so and we would like you to go and see your insurance company doctor to have a medical and get more insurance. Then we'll talk about it. He went to his doctor and the report was given to the insurance company. A week later his report came in and said that he had not qualified for the extra insurance and no one, not the employer, not the insurance company nor the doctor, no one would tell him why. He was not told why he did not qualify and he of course immediately assumed that he was dying of something horrible. So, we just kept putting pressure on. You know, phoning people, going through B.C. Medical and the doctor and so on.

Who disclosed it eventually?

The doctor, finally.

To the patient?

We said, look we're not asking you to tell anyone but the man whom it concerns. Then, of course, another example that I remembered about information being sold was when the B.C. Government Motor Vehicle Licence Bureau sold our plate numbers and all of our addresses to an insurance company who had approached us ..... and that happened in B.C. here about, what'd it be, about seven or eight years ago, Doug?

I don't remember now.

In all of those things, it seems to me that what we're looking at here are contradictions. On the one hand you have a section in the Credit Reporting Act which says that the doctor can quite nicely keep information about you, yet here we are wanting to have the other side. So, I think we have a bit of a dilemma there that we're going to have to really look at.

The other thing that I had on my next card has already been mentioned as well, and we talked about supermarkets and department stores having the automated computerized checkouts where they've got scanners and DTS. And I thought it was very interesting when I saw the very first tape that came through a scanner - it had the exact time of day, it was 5:27 sort of thing. It wasn't just, you know, the time of day, the afternoon or something, it was that exact moment that it went through. It seemed to me that at that stage of the game, I knew I was accused of being slightly paranoid, but it struck me that the potential was there to be able to check buying patterns and to get back to the suppliers and tell people. All in the good name of checking inventory, of course, but if you really wanted to get paranoid and start postulating you could say that there could be quite a good manipulation of stock. In other words, if you went in and wanted to buy bulk rolled oats, we'll say, in a 5-pound sack, that was inexpensive because it did not have a lot of packaging and so forth, but where the demand wasn't very high, that could nicely disappear from the shelves. The other thing of course, is that many people now are able to buy groceries or any products, for that matter, with credit cards, and the new computerized machines put the cheques in and they have a special identity number for cheques and all the rest of it, so, certainly they have access to your records.
Another area that we are concerned with is the electronic funds transfer system and this, of course, is another horror story and we don't see, so far, any provision of easy access for making corrections of computer errors.

On computer related errors, you have the situation where you have automatic deposits from payroll, for example. There was a court case last year, where this fellow was dealing with a particular bank that was depositing his pay cheque for

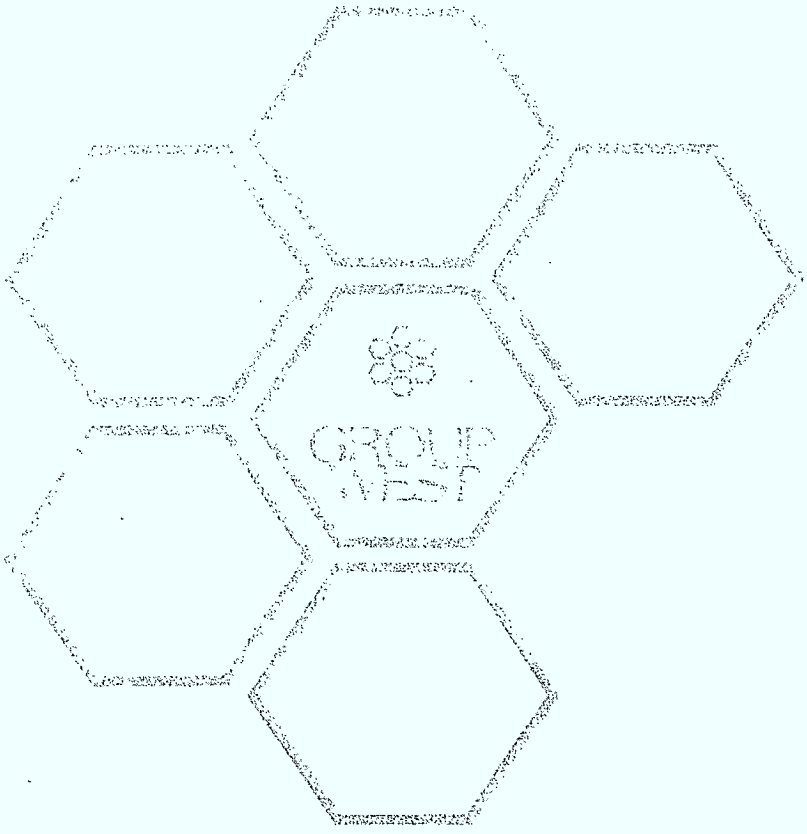
his mortgage. Every month he had made arrangements for his mortgage payments to be put through on a certain date and pretentiously, for two years, every month, two days before that payment was due, they put through his mortgage payment so that he was overdrawn and they charged him interest. So he went to court and finally won the case. We did a computer study in conjunction with Simon Fraser Computer Science people a couple of years ago, where we canvassed our C.A.C. members. We have no political affiliation, we are a non-profit, volunteer, non-partisan group and so it's an open membership. We take all comers so we think that it's a pretty good cross-section. Of those people contacted who were asked if they had had a computer related error in either their credit or charge card billings, or in their bank accounts, 54 percent of those people reported a computer related error. So generally we're worried about safeguards being built in to insure privacy and that there is not access, again, to personal information as we've defined it here. Certainly I would subscribe to that information. I think that perhaps the best way to try to insure that there is something done about this is to have input from "consumers", the users, the end user of the system and not just to have people in Toronto deciding.

The discussions relating to advocacy groups focused on the use of private information to impinge on human rights. This was particularly important where personal medical or work histories were used without the knowledge of the individual. While this was not related directly to Videotex, it did illustrate the danges inherent in broader based data banks with controlled user access.

A second issue related to the need for citizen and consumer advocacy groups to be included in the planning and implementation phase of services, such as Videotex. This was considered critical to allow consumers a voice in the design and development of systems. The importance of encouraging wide access and openness in system implementation and equitable development was also stressed. Through representation and the fostering of an open accessible system, it was felt individual rights and protection of privacy would be facilitated.

The implementation of a regulatory body to deal with issues of information use, technical standards and system implementation was also discussed. Other areas for regulation included security and aspects of privacy. The problems of implementing a regulatory body stem from the changing nature of the technology and that, at present, the issues are only emerging. Public sentiment and political action are only now being aroused with respect to the implications of data communication systems. It is also clear, that laws and regulations can not only be limited to Videotex but must include a range of services.

A final area of concern focused on the ability for individuals to edit data files of their own records. It was recognized that large amounts of data are regularly collected from several sources. The security of those files and the use of those files is outside the control or jurisdiction of those supplying the information. The implication of such a situation is that people loose the right to the uses of their own information and are therefore under the control of those holding the data. There is, as a result, a need to increase the public awareness of such files and to educate the public about their rights to information.


GROUP
WEST

PRIVACY WORKSHOP - PROPOSED PARTICIPANTS

1. Rex Schoffield - Vice President, Dominion Directory, Member of VISPAC. Active as a major Information Provider to B.C. Telephone. Mr. Schoffield will discuss the maintenance of internal records of customer accounts from the IP perspective.

2. George Fierheller - President and Chief Executive Officer Premier Cable. Mr. Fierheller will present the Cable industry's viewpoint on regulation and privacy and the role of the cable company in the provision of services for Teledon.

3. Peter Booth - Director Research Group West. Mr. Booth has involvement in several areas of Teledon activity. He is directing the N.B. Tel field trials as well as assisting in the design of Bell Canada's trial. In addition, he is currently conducting a major feasibility study for B.C. Tel. Mr. Booth will address the issue of secondary uses of data.

4. Jean Douglas - Consumers Association of Canada. Mr. Douglas will be presenting the views of her association on the role of computers and the consumer. Individual rights and the impact on the consumer are to be discussed.

5. John Olsen - Director, Information Service, Provincial Government, 1975.
   - Organizer of the first B.C. Community Communications Conference.

6. Val Embree - Graduate Student, UBC Health Sciences. Ms. Embree has a strong background in Human Rights Legislation having worked in a Government Agency investigating case discrimination. She will address the issue of unequal access, the use and abuse of the pre-employment medical.

7. Gil Evans - Co-ordinator of the Greater Vancouver Information Referral System. Mr. Evans will discuss the structure, controls and format of community information bases, and how Teledon might effect them.

8. Rod Booth - Television and radio producer and broadcaster, Director of Communications, B.C. Conference of the United Church of Canada. Mr. Booth will express the Church's concern about the covert accumulation of information.

9. Doug Seeley - Lecturer, Computing Sciences, Simon Fraser University. Dr. Seeley is a well known researcher in the human use of computers.

10. Jackie Kelly - Lawyer, Davis and Company. Ms. Kelly has specialized in the research of Computer Law.

11. L.M. Bewley - Associate Professor, Library Sciences, UBC. Prof. Bewley's specialized in legislation regarding Public Library Services. She will address the issue of the creation of software and the potential for manipulation of information within the data base.

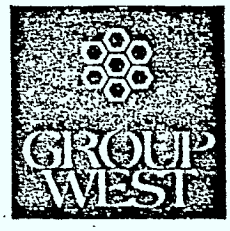
12. Lorne Nicholson - MLA, B.C. Provincial Government, Science and Communications critic.

13. Neil Hunter - Pastor, Fairview baptist Church. Rev. Hunter is an outspoken critizer's advocate, active in the World Council of Churches and Vancouver community committees.

14. Scott Gardiner - GAMMA Group, Montreal. Author of paper entitled Personal Data Banks and Personal Autonomy.

15. Garth Brown - Canadian Labour Congress, Regional Co-ordinator. Mr. Brown will present the views of his organization with respect to the role of computer services and data banks with respect to the labour force.

16. Mike Aysan - Vice President, Manitoba Telephone Company and head of Project IDA. Mr. Aysan will discuss the ongoing Teledon trial and the issues which have developed in the provision of privacy to trial participants.



WORKSHOP

ON

PRIVACY IN VIDEOTEX

THURSDAY, MARCH 12, 1981

SUITE 500, 1148 HORNBY STREET

VANCOUVER, B.C.

5th Floor, 1148 Hornby Street, Vancouver, B.C. V6Z 2C4 (604) 687-2355

AGENDA

9:00 a.m.

WELCOMING ADDRESS

P.J. Booth
Director, Group West Research

9:10 a.m.

INTRODUCTORY REMARKS - CHAIRMAN

John Olsen
Appropriate Technology Consultant
Unicorn Services

9:20 a.m.

PRIVACY AND THE INDIVIDUAL

Aside from the effect of electronic technology, how do people feel about privacy? What kinds of information do they consider private? Are there ethical or moral values that people hold to be immutable? How should privacy be defined?

Rev. Neil Hunter
Pastor, Fairview Baptist Church

Scott Gardiner
GAMMA Research

11:00 a.m.

GATHERING PRIVATE INFORMATION

How may the system be designed to protect privacy? Who should gather the information? What kinds of private information should a Videotex system handle? Should the consent of the individual be required? Who owns private information once it is gathered?

David Godfrey
Department of Creative Writing
University of Victoria

Lois Bewley
Associate Professor, Library Sciences
University of British Columbia

12:30 p.m.

Hosted Lunch

1:30 p.m.

PROCESSING AND STORING PRIVATE INFORMATION

Can the private information be altered or misrepresented? Who might have access to it? When and how should purging of information take place? Who owns the information? What is the extent of Cross-referencing which should be allowed.

Doug Seeley
Lecturer, Department of Computer Sciences
Simon Fraser University

Rex Schoffield
Vice President
Dominion Directories

3:00 p.m.

DISSEMINATING PRIVATE INFORMATION

Can an information seeker obtain data to which he or she is not entitled? Can private information be sold? Who will make the laws effecting privacy? Who will monitor and enforce them?

Jackie Kelly
Davis and Company
Specialist in Computer Law

Peter Booth
Director, Group West Research

Jean Douglas
Consumers Association of Canada

5:00 p.m.

Summary - John Olsen - Chairman

5:30 p.m.

Refreshments

VIEWDATA AND PRIVACY

AN OVERVIEW

PREPARED FOR THE

WORKSHOP ON PRIVACY

IN

VIDEOTEX

VANCOUVER, MARCH 12, 1981

P.J. BOOTH
FEBRUARY, 1981

ACKNOWLEDGEMENT

The author gratefully acknowledges the contributions to this paper of Donna Moffat, Dorothy Phillips and Teresa Plowright.

This paper presents an overview of some of the issues which are relevant to understanding the impact of innovations such as Videotex on society and the individual. The particular focus is on the issue of privacy and Videotex services. The paper proceeds by initially supporting the need for the humanist perspective in understanding technology and its role in society relative to man. Then a review of past activity by the Computer Task force sponsored by the Department of Communications is presented. The final sections deal with a number of specific issues relating to the concept of privacy, exclusion and secondary uses of data. The need for further discussion of the issues by all interested parties involved with Videotex is supported through the conduct of the proposed workshop on privacy.

INTRODUCTION

The development of computer linked telecommunications devices such as Videotex or Telidon has opened the door to numerous discussions relating to the macro and micro issues inherent in its development, and to society's acceptance of that innovation. Issues are now being raised which address the concerns of social policy, regulation and legislation. This has been manifest in the realization of the need for the development of government policy with respect to the processing, handling, storing, carriage and brokerage of information generated by computers generally and Videotex in particular. There is no doubt that issues relating to the development of this service are current, and highly relevant to the data communications industry and society in general. Areas which require further investigation, or at the least consideration, are current regulation, existing legislation, social policy, technological capabilities, standards and societal norms or expectations.

Speculation about the direction this new innovation will take and its consequent effects have been made by numerous researchers and industry practitioners. These range from the optimistic views of the futurists with visions of wired cities, electronically managed living environments and spatially altered landscapes to the pessimistic views of psychologists about the inherent dangers of alienation and the desocializing effects resulting from the reduction of face to face contacts. Others have raised the issues of centralized information control, and the spectre of an Orwellian society where individual rights and freedoms are minimized and automony ceases to be possible. In such a society

the individual is controlled by the machine and those in positions of power reach out and influence the citizen through the technology.

The divergent opinions about Videotex are often difficult to reconcile and to forge into a coherent scenario for future developments. There is, it seems, no denying how engaging the technology seems to be. There is a blend of innovativeness and appealing application which can meet some very gratifying ideals for managing society. Such innovations aid in bridging the gap between the physical elements of human behavior and existences and the nosphere or knowledge sphere of human thought. The reality of the present state of development requires the consideration of those elements which will, to a great extent, influence, the ability of society to adapt to these innovations, the capability of individulals to alter their behavior and to perceive such innovations as effective and useful tools for everyday life. The infrastructures which are developed, and the institutional frameworks which are set up are an integral part of the orderly development of such a technology. Fundamental to that process is a need to minimize the negative impacts resulting from the innovation on individuals and society.

Ellul (1964) has elicited similar concerns in a philosophical context by stating the need for an understanding of the humanist perspective in a rapidly accelerating technological world. A critical element is the need for bringing technology and man together in the development stages of an innovation, rather than juxtaposing one against the other in the production and operational stages. In a rather

Hegalian or dialectic view, the two elements should be considered equally important and closely linked to ensure an equitable development with the minimization of negative effects on society.

BACKGROUND

In 1971, the Department of Communications and the Department of Justice issued a report on Privacy and Computers. That report was part of the Task Force on Computer Communications set up to aid in ensuring the orderly development of communications in Canada. The Department of Communications was interested in two issues:

- Assessing the probable consequences of current and future communications technology.
- Identifying the social and economic needs which might be met by Communication Systems.

The advent of Telidon and the range of services broadly defined as Videotex has created a renewed interest in the issues focusing on the social consequences of computer services. A central focus of that concern is the issue of the social and psychological impact of Videotex on the individual and society. Within that broad paradigm, the issue of Privacy represents a central focus. Privacy issues have been identified in two contexts:

- Primary Uses of Data; Banking, Messaging
- Secondary Uses of Data; Billing Records, Access, Tracking

In previous studies dealing with Privacy and Computers, the D.O.C. Task Force (1975) outlined the criteria needed to minimize threats to individual rights:

"It must provide security and protection of privacy in the areas

of: data acquisition

data storage

data dissemination"

In the areas of acquisition, all information relating to the individual must be sanctioned by the subject, him or herself, except where such information is seen to be of importance to the public, ie: police records. The subject must have access to the data acquired for verification, be advised of how and by whom the data was acquired and how they may be used. Furthermore, those authorized to collect data must be bound by legal and professional constraints in what data they collect and how it is collected.

In the area of data storage, methods by which mechanical and human error may be identified must be devised. Provision must be made for the updating and purging of data by personnel bound by legal and professional constraints. The very quality of storage must be assessed to ensure the data is protected from deterioration or illicit access.

In the area of data dissemination, the owner/subject must be identified and given access to verify data and sanction item sharing. The reliability of all data and computer analysis should be assured before dissemination.

An overriding need for data communications is the development of legislation to enact laws which protect the rights of individuals and which codify the precedures outlined. For the development of the legislation, standards of performance must be defined along with a realistic assessment of enactment and enforcement. There are as well major problems of jurisdiction and definition which need to be addressed.

CONCEPT OF PRIVACY

The current evaluation of the concerns relating to Privacy and Videotex is designed to address a range of issues relevant to the individual and society generally. In Gotleib's (1978) review of the effects of computers in the home, a critical impact was identified as access to information control and security. It was suggested that the most significant problems for this innovation will be:

- Jurisdiction
- Licensing
- Content

In discussing the public acceptance of the service, privacy was identified as a major issue:

> "Will questions about confidentiality and privacy, and doubts about changes in lifestyle add to the concerns of a public that is increasingly unsure about the enveloping influence of computers" (Gotleib, 1978, p. 25).

Cardell (1975), in assessing the impact of computers on society suggested that we are at a critical stage where a number of important decisions will be made on

how technological innovations develop. An overriding concern was specified as the degree to which man as social being can achieve full control over his own life situation. In maintaining privacy, the fundamental concern rests on preserving individual freedoms and fostering the development of new technologies in such a way they contribute to the realization of positive social goals. Failure to do so, it is suggested, may lead to a further isolation and powerlessness which too many people already experience in society.

The issue of privacy has also been raised by Gardiner (1980) in his discussion of Data Banks and Personal Automony. In that discussion, Gardiner examines the issue of privacy at the individual level and considers issues from a psychological perspective. A fundamental point is the distinction between privacy or loss of privacy and the erosion of automony. The basis of Gardiner's distinction lies in what he refers to as the degree of control individuals have with respect to the accumulation and dissemination of information. In a sense, that control represents the degree of self-determination an individual has with respect to data which may be used to gain knowledge about him or herself by other individuals. It is the loss of that control which represents according to Gardiner, the threat to the individual so inherent in the accumulation of central data banks.

In assessing Gardiner's viewpoint, two important concerns become evident. One is the types of data individuals disclose about themselves in various societal transactions. Such transactions are, for example, an application for credit or the

accumulation of data under a SIN number. Second is the secondary use of such data and the facility for cross referencing data sets to form profiles. Common thought tends to view the second point as the fundamental evil. Gardiner's view is that the creation of central data banks equate to a loss of personal automomy, and hence facilitate the invasion of privacy. However, just as Gardiner illustrates that Privacy is a relative term, so to issues of automony and control must be viewed relatively. The issues of societal norms and expectations must be examined to illustrate the extent to which individuals feel a loss of automony. Clearly in many minds, living in a technological society requires the acceptance of a certain degree of impact on lifestyles and freedom of choice. The important issue, however, may be the assessment of where on the continuum between the total loss of automony and a pristine world of full self disclosure, our society will develop. As well, the need exists to ensure that whatever degree of personal rights and self determination are considered acceptable they are equitable for all members of society.

EXCLUSION

Related to privacy and automony is the issue of exclusion. Exclusivity may be viewed in terms of information not stored in data banks and, as well, in terms of the restriction of access, or more correctly, the exclusive access of some to specific data files. For those with access, the power to construct data profiles increases while each individual has less control over the uses of such data.

The development of data files which are controlled by a few individuals and accessable only to a select group presents a situation where an individual's behavior, conduct and characteristics can be observed and henced utilized in a variety of covert ways. Such actions present a definite threat to the rights of an individual and represent the intrusion of privacy.

SECONDARY USES OF DATA

The issue of cross-referencing and secondary data uses in Videotex may be examined within two contexts. One is the cross-referencing of different data bases comprising the various Videotex functions. The second is the cross-referencing of files resulting from the use of a Videotex system. Such files will contain records relating to a variety of user choices and characteristics. The collection of such information will most likely be in the hands of system operator and could involve the network supplier, as well as large centralized Information Providers.

The cross-referencing of information within a Videotex data base is of minor concern to the issues of privacy. Such manipulations merely allow the connection of one page of information to another. It has recently be suggested that Videotex systems should have unlimited cross-referencing by which it would be possible for the information provider to direct the user from one page in the database to any other page. Such facilities allow the database user to move around the database with the maximum speed and efficiency.

The most important concern relative to the privacy issue is the cross-referencing and access of user data files. Consideration for the user of Videotex files has received some attention from Information providers and the Department of Communications. The Information Providers Association (VISPAC) addressed the issues peripherally in its code of ethics.

Article (5) "Where an Information Provider offers direct purchase of goods or services using the two way facility of a Videotex system, the user may be in no doubt as to the consequences of using response frames with respect to financial obligation thereby incurred or to voluntary disclosure of private information."

Article (10) "No Information Provider will collect or cause to be collected any data or information about a user which is not necessary to the specific conduct of the Information Providers Videotex or Teletext operations, and no Information Provider will disseminate any such information or database that a user may be identified or his or her privacy violated, without the expressed consent of the user.

In each of the articles outlined, the right of an individual to be aware of uses of specific data is defined. In each case, the implications for invasion of privacy are presented to the individual. The individual is then given the knowledge that the information may be used in some manner. The actual extent of use,

however, remains undefined. The choice an individual has in such a situation is limited to not using the system or not utilizing a particular service or system feature. The important concern remains the definition of the extend of secondary and tertiary use of such information.

The Department of Communications has considered the issue of privacy in terms of the secondary uses of data gathered in Telidon field trials. The guidelines for data collection include:

1. Each user of a Telidon should be assigned an account identification (AID) number different from the users account number. All data used for secondary analysis should be labelled with the AID. The same AID will be used for demographic and other data so researchers may relate questionnaire and usage data without knowing the identify of the source of the data.
2. Researchers or users of data will publish data only when it has been aggregated over enough people so that individuals cannot be identified.
3. Operators will make users aware that usage will be monitored for research purposes and will ask the user permission to monitor.

The D.O.C. guidelines emphasize the need for ensuring the anonymity of participants in the Telidon field trials. Those guidelines also suggest possible methods for limiting the covert uses of information in actual Videotex operations. Prime importance rests on restricting the tracing of usage and the identity of individuals for purposes other than necessary for the operation of a

Videotex system. In secondary and even tertiary uses of data, Videotex users would frequently be unaware of the activity. An important concern therefore, is the need to provide full disclosure of all phases of data usage to an individual. Such disclosure could be provided when the potential subscriber is contracted for service.

The important questions required for investigation include:

- The conditions under which we should allow different types of information concerning an individual to be collected.
- The structures which should be developed to ensure equitable treatment of individual data records.
- The constraints which should be placed on the storage and cross referencing of information.
- The limits which should be defined on the disclosure and uses of stored records.
- The definition of rights of access and non-exclusion with respect to data which has been collected.

CONCLUSIONS

Each of the issues are important to all parties involved in the development, use and control of information services such as Videotex. That includes:

- Government
- Industry
- Citizen Representatives/Advocacy Groups
- Academics and Practitioners

Development of a perspective on the issues relating to privacy and individual rights requires the input of representatives from each of several areas.

- Those involved in developing policy and legislation
- Those dealing with legislation and jurisdiction
- Representatives of advocacy groups and advocates of citizen rights
- Representatives from business involved in the various areas of service provisions
- Individuals representing the moral and ethical views of society
- Representatives from the information service business and those involved in technical development

Issues need to be examined within each phase of Videotex development and operation that includes:

1. Data development - Information page creation
2. Data storage and user file creation - Primary file usage
3. Data dissemination and secondary file usage.

BIBLIOGRAPHY

Department of Communications. Telidon Aggregated Statistics. Department of Communications/Government of Canada, July 1980 - Ottawa.

Ellul, Jaques. The Technological Society. Vintage Books, Random House, N.Y. 1964.

Gardiner, S. Personal Data Banks and Personal Autonomy. Science Council of Canada, Ottawa, 1980.

Gotleib, C.C. Computers in the Home. What Can They Do for Us - And to Us. Institute for Research on Public Policy, Ottawa, 1978.

Halina, Jos. W. Communications and Communities. A North American Perspective. International Commission for the Study of Communications Problems - Unesco, 1978.

Jordan, F.J.E. Privacy Computer Data Banks. Communications and the Constitution. Privacy and Computer Task Force - Ottawa, 1975.

Pergler, P. The Automated Citizen. Institute for Research on Public Policy - Montreal, 1980.

Plowright, T. Social Aspects of Videotex Services. Proposed Research Directions. Social and New Policy Division, Broadcasting and Social Policy - Federal Government of Canada - Ottawa, 1980.

Royal Society. Communications into the Home. Royal Society of Canada, Ottawa, Canada, 1972.

Secretariat for the Future. Man in the Communications System of the Future. Stockholm, Sweden, 1975.

Sharp, J.M. Regulatory Models. A Study for the Privacy and Computers Task Force. Department of Communications, 1975.

VISPAC. Draft Code of Ethics. Videotex Information Providers Association of Canada. Ottawa, 1980.

PERSONAL DATA BANKS AND PERSONAL AUTONOMY

a paper submitted to

SCIENCE COUNCIL OF CANADA
100 Metcalfe
Ottawa

by

W. LAMBERT (SCOT) GARDINER

of

GAMMA
3535 Queen Mary
Montreal

on

31 AUGUST 1980

TABLE OF CONTENTS

CONVENTION: So that the argument in the text can be as clear as possible, the usual clutter of comments and citations is moved to the end of the paper. The former are indicated by letters in brackets and listed under "notes"; the latter are indicated by numbers in brackets and listed under "references".

1 FROM PRIVACY TO AUTONOMY

Most discussion of the psychological effect of personal data banks (that is, those containing information about a person beyond that which the person chose to make part of the public record - like publications and interviews) has focussed on the issue of privacy. The Information Privacy Research Center at Purdue University had a bibliography of 2,500 items in early 1979 and the flood of empirical studies, theoretical discussions, Commission reports, popular books has continued to flow since then (11). It is an important issue. Here, however, I would like to go beyond it to what I consider a deeper issue (a). My argument is that the major threat of personal data banks is not invasion of privacy but erosion of autonomy.

First, a few words in support of the shift from the issue of privacy to that of autonomy. Privacy is a relative term. It varies from individual to individual. Some of us define it as not being seen, some as not being heard, and some as not being known. Some of us define it the other way round - not having to see (a flasher, for instance), not having to hear (a neighbour's Rolling Stone record at 3 a. m.), not having to know (a stranger's problems during a trans-Atlantic flight). It varies from culture to culture. In some Third World countries, the ground floor street-side apartments are most expensive, since members of that culture value conviviality over privacy (b).

2 SELF-DISCLOSURE AND IMPRESSION MANAGEMENT

Let us consider two related concepts in the psychological literature - self-disclosure and impression management. Self-disclosure is the open and honest presentation of one's self, whereas impression management is the creation by a person of some desired impression on other people. Those concepts are related not only to one another but to data banks, on the one hand, and to autonomy, on the other hand, and will thus serve to link data banks to autonomy.

The principal advocate of self-disclosure was Sidney Jourard (5, 6). Being a therapist, Jourard aspired to encourage self-disclosure in his clients and found that he could indeed help create a climate for self-disclosure by practicing self-disclosure himself. However, he found that, even in the therapeutic situation which is explicitly designed for self-disclosure, there was a great deal of impression management.

Our initial reaction is probably to favor self-disclosure over impression management. However, perhaps people have good reason to "disclose" to strangers in trains and planes, to group therapists and marriage counselors in the next town, and to local therapists and priests, only on the understanding that the information is confidential. They know that knowledge is power

people who can tailor their social behavior to each situation, and low self-monitors, who view themselves as open and honest people who prefer self-disclosure to impression management. Those two views are based on different concepts of the self - the low self-monitor believes that there is one self which should not vary from situation to situation whereas the high self-monitor believes that there are many selves which differ from situation to situation.

no effect on behavior unless the person perceives it, whereas a mugger that the person imagines to be lurking behind the tree will have an effect on behavior. The unperceived tree is part of the objective world but not of the subjective map, whereas the imagined mugger is a part of the subjective map but not of the objective world.

The central element within the subjective world is the self-concept - that is the person as that person sees him/herself. The most important aspect of autonomy is control of one's self-concept. We tend to think that this self-concept is discovered. This assumes that there is some "true" self that one gradually discovers. The evidence however is that it is an invention. Each of us invents our self. We vary in the degree to which this invention is an authentic expression of our growing from the inside out or a social fabrication based on our conditioning from the outside in. Those with an internal locus of control tend to the former and those with an external locus of control tend to the latter.

A single series of numbers for all citizens is a useful adjunct to such a data bank. The Social Insurance Number (SIN) is such a series. Once again, the argument is convincing. It helps make social services more efficient. However, it is now used by some schools and universities as a student number. Thus, some one who has chosen to stay out of the paternalistic system is forced, if he wishes to attend such schools, to acquire a Social Insurance Number (g).

The storage capacity of computers is making the compilation of huge bodies of data technically feasible. The Personal Chip which not only identifies us perfectly but also locates us is already here (2). We are familiar with being uniquely identified by our fingerprints but, unless we stray, need not get on to that file. We are already familiar with personal locators when we realize that anyone could follow our activities through the trail of credit card bills we leave in our wake but we can choose not to use such credit cards (h). However, we are not yet sensitized to a system which does this so efficiently, and with the pressure to adopt such a system in a pragmatic society, which tends to assume that what <u>can</u> be done <u>should</u> be done. "Invention is the mother of necessity."

irritation to a constant concern. Remembering the importance of the subjective map (see Section 3 above), it does not really matter whether the person does so or not. If you think that the person may have done so, then your perceived locus of control is made more external. You are pre-judged when you meet.

5.2 Some of us are famous

Some of us are famous. That is, are known - or, rather, are known of - by many people that they do not know. Famous people often have identity problems because so many people pre-judge them on the basis of their record rather than of their personality (i). This pre-judgment could be considered as a precise prejudice. That is, the person is not pre-judged because of certain superficial attributes - black skin, woman's body - but because of his/her public image.

Personal data banks make us all famous. We are all famous not so much in the manner suggested by Andy Warhol that everyone in our modern media-saturated world can be famous for five minutes but in the sense that we are all potentially knowable in fifty seconds (j). That is, anyone who wishes to do so and has access to the personal data bank can know of us even though we do not know of them. Most famous people choose to establish a public record (and many of them work hard to build it) and are willing to pay the price of fame. Many of us choose obscurity

5.4 Some of us live in total institutions.

Some of us live in total institutions. Many of us are critical of the donning of masks and the playing of roles off stage. However, Goffman argues that the de-humanization in total institutions (prisons, mental hospitals, etc.) is partly due to the fact that our "props" are taken away and, with them, the very human right of representing our selves as we wish (4).

Personal data banks could have a similar effect. They would not take away our masks and our costumes but they could make them transparent. If another person could meet us on paper (so to speak), by consulting a data bank about us, before meeting us in person, then our capacity to manage our impression is very much limited. In a classic study on impression formation, a guest lecturer was presented to half the class as a "rather cold person, industrious, critical, practical, and determined" and to the other half as "a rather warm person, industrious, critical, practical and determined" (7). The "warm" subjects liked the lecturer better and volunteered more in the class discussion than the "cold" subjects. If the simple substitution of "warm" for "cold" can have a significant impact on the subsequent impression, then the increasingly more extensive information in a data bank could result in a pre-judgment which a person would have difficulty in changing.

Regulation should cover not only those who make withdrawals from such personal data banks but those who make deposits in it. What comes out is a function of what goes in. Since those who put information in tend to be bill-collectors for private firms, public agencies dealing with problems, and so on, the information which goes in and thus the impression that comes out tends to be negative. Family and friends should be solicited as information providers to add some positive information. The fear of exploitation by faceless, nameless people who tend to use those data banks is perfectly justified. Philip Zimbardo, in his studies of de-individuation, has clearly demonstrated that people who are unidentified will treat others much more unkindly (15). Stanley Milgram, in his studies of obedience, has shown that we are more likely to hurt someone when we cannot see them (10). Thus, whereas we would not say something negative about a person to his face or even to another person, we would not hesitate to deposit it in a data bank.

Public policy will differ when one is concerned with the erosion of identity than when one is concerned with the invasion of privacy. The important issue is not so much what "private" information is available but how much control the person has over the accumulation and dissemination of this information. The basic principle should be that, except in extreme circumstances when a person has clearly demonstrated lack of responsibility and thus

NOTES

a I am indebted to Dr. Arthur Cordell of the Science Council of Canada for this suggestion.

b The difficulty in translating the word "privacy", even within what linguists derisively called Standard Average European, suggests that it may just be an Anglo-Saxon aberration. Anyway, in those enlightned times, who can even talk of "private parts" without smiling?

c "Open and honest" may initially appear redundant. However, "open" refers to the capacity of a person to disclose all of themselves and "honest" refers to the capacity of a person to be truthful in whatever they choose to disclose. The first term covers sins of omission and the second term covers sins of commission. Hence, a complete data bank would contribute to openness and an accurate data bank to honesty.

d People may choose, for example, to disclose themselves in their intimate relationships and manage their impressions in their contractual relationships (9). This distinction, by Salvadore Maddi, can be illustrated by a person buying groceries for his mate. His relationship with the grocer is contractual. It does not really matter to him that this particular grocer stocks and serves the goods and to the grocer that this particular customer selects and buys them. However, it does matter to his mate that he cooks dinner for her and to him that he is doing it for her. His relationship with his mate is intimate. The participants in the relationship are not interchangeable. Part of the understanding in such a relationship is that one discloses oneself, since it is that unique self which is involved in the relationship. Part of the understanding in the contractual relationship is that one plays one's role and reveals only that part of oneself which is appropriate to that role.

e Actually "social class" also correlated. However, this is probably because "social class" is also correlated with "destiny control". Lower-class children tend to perceive themselves as having less control over their lives (partly, at least, because this is true - they do indeed have less control over their lives).

f Science fact writers tend to put down science fiction writers. However, the better science fiction writers have had a better record in predicting the future than most academic futurists. They do serve to provide as with various lucid visions of desirable and undesirable futures.

about her. The electronic data terminal started stuttering out a series of citations.

SHE: A computer in California knows about me? That's strange and scary.

ME: Read the citations. Is there anything there which you did not know were part of the public record?

SHE: No. They are just reviews in the Montreal newspapers of my dance performances.

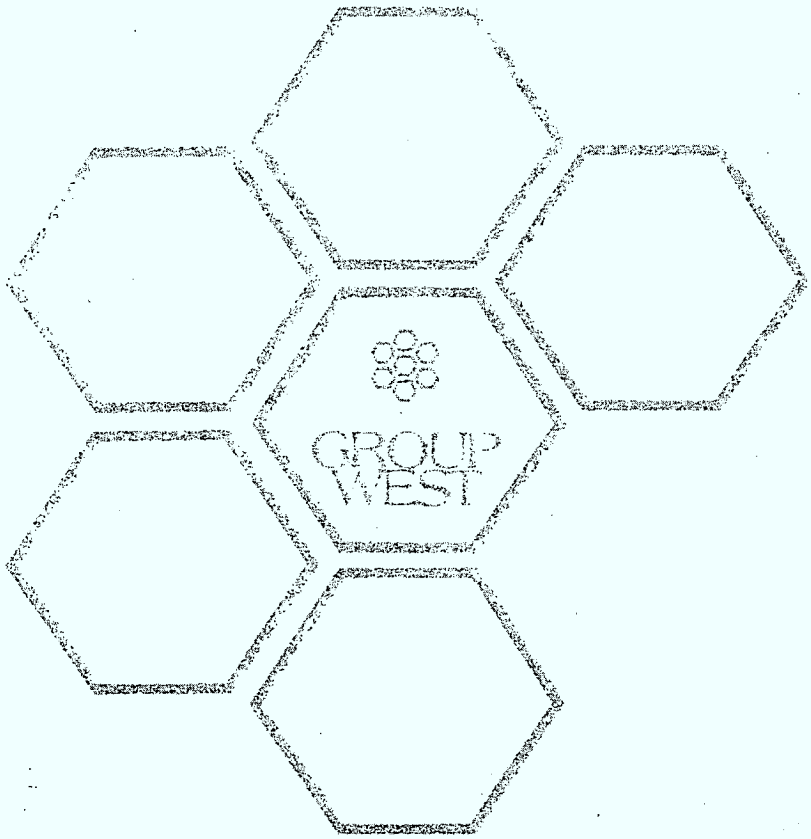
ME: Then, why is it scary? You knew that this information is available.

SHE: I knew that it was available - but I did not know that it was so accessible.

k The Horatio Alger myth which inspired North American society is challenged by the Conserver Society, which questions "fortune" as a goal, and the Information Society, which questions "fame" as a goal.

l The Catholic confessional contributes to the human need to shed burdens of the past. Protestant guilt, on the other hand, accumulates day by day throughout a lifetime, building capitalistic Empires outside and bleeding ulcers inside.

m Try, for example, to get any information about the Royal Commission on Confidentiality by calling Horace Krever at (613) 965-4003.


GROUP
WEST

--BOOTH, P.J.
--Privacy in videotex : a workshop conducted March 12, 1981 Vancouver summary report.