



Communications  
Canada

QUEEN  
K  
3264  
.C65  
P75  
1991  
c.2

*strategic*

*policy*

*planning*

■ ■ ■

*planification*

*stratégique*

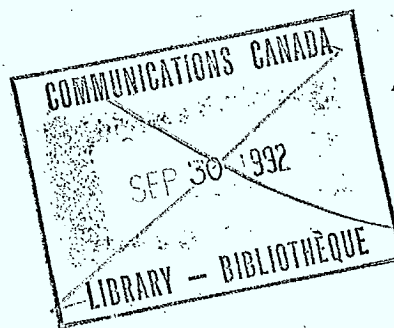
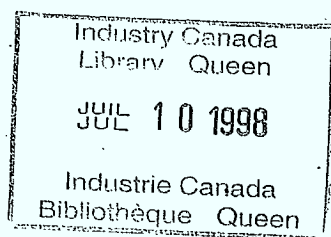
*des politiques*

12  
**PRIVACY AND DATA PROTECTION  
STRATEGIC PLANNING WORKSHOP** 00

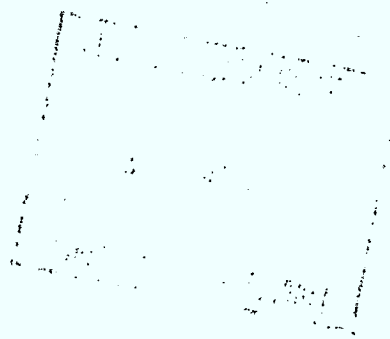
S  
T  
R  
A  
T  
E  
G  
Y  
  
A  
N  
D  
  
P  
L  
A  
N  
S

STRATÉGIE ET PLANIFICATION

11  
**PRIVACY AND DATA PROTECTION  
STRATEGIC PLANNING WORKSHOP 00**



**REPORT ON THE WORKSHOP  
HELD ON DECEMBER 5, 1991,  
GOVERNMENT CONFERENCE CENTRE  
OTTAWA, ONTARIO**



DD 12018634  
DL 12038718

K  
3264  
C65  
P 75--  
1961  
2.12

---

### ACKNOWLEDGEMENTS

The Strategic Planning Workshop on Privacy and Data Protection benefited from the participation of many individuals from the Department and outside agencies and organizations.

I would particularly like to thank the Director General, Strategy and Plans, **Eileen Sarkar**, who agreed to chair the Workshop and to those individuals that participated as speakers in the day's program. I would like also to thank those who lent their support to the idea of the Workshop and many useful suggestions regarding the agenda and speakers.

Special appreciation goes to those who planned and organized the day - **Brenda Patterson, Stephanie Perrin, Suzanne Loranger and Suzy Beauregard.**

And finally, I would like to thank all those who attended the Workshop for their interest and encouragement as together we considered and explored privacy and data protection issues challenging DOC. The Workshop would not have been a success had DOC employees not taken the time to share their ideas and opinions on these matters.

David Waung  
Director  
Strategic Policy Planning

---

---

## TABLE OF CONTENTS

Executive Summary .....	4
Introduction .....	6
Keynote Speaker .....	6
Panel Discussion : <i>Defining the Issues</i> .....	9
Luncheon Speaker .....	13
Panel Discussion : <i>International Influences and Developments</i> .....	13
Panel Discussion : <i>Technology, Legislation, Codes of Conduct</i> - What are the Answers? .....	15
Chairperson's Closing Comments .....	18
Appendix 1 - <i>Registered Participants</i> .....	
Appendix 2 - <i>Workshop Agenda</i> .....	
Appendix 3 - <i>Privacy - The Issue</i> .....	

*The following Background Papers are also available upon request  
(please note, in language of author only):*

NEW YORK STATE PUBLIC SERVICE COMMISSION PRIVACY PRINCIPLES  
CANADIAN STANDARDS ASSOCIATION PROPOSAL FOR A MODEL PRIVACY CODE

---

### EXECUTIVE SUMMARY

The Department of Communications Strategic Planning Workshop of December 5, 1991 entitled, Privacy and Data Protection, considered the various forces and developments which are influencing issues and trends in privacy and data protection. Of particular concern were the strong linkages between the sophistication and use of communications technologies and apparent opportunities for privacy infringements.

It was emphasized many times during the Workshop that privacy is a universal moral value. However, it also appears that our ability to maintain and control our right to privacy is seriously threatened. The increasing ease with which information is collected and manipulated, and the economic value inherent in "information" are infringing on our privacy expectations.

It was suggested that these developments require an explicit and appropriate benchmark defining an acceptable level of privacy protection. Participants were told that our expectation for privacy has several different dimensions:

- SOLITUDE - THE RIGHT NOT TO BE DISTURBED
- INTIMACY - THE RIGHT NOT TO MONITORED
- ANONYMITY - THE RIGHT NOT TO BE KNOWN
- RESERVE - THE RIGHT TO CONTROL ONE'S PERSONAL INFORMATION

Workshop discussion explored the apparent conflict between economics and technology and social values such as privacy. The suggestion was made that our privacy expectations must inevitably change in response to economic and technological changes. This however was challenged by those who argued that the public should not be coerced into diminishing their

challenged by those who argued that the public should not be coerced into diminishing their privacy expectations. The goal should be to strike balance between the conflicting demands of economic efficiency and technological innovation and social values such as privacy.

Many of the speakers noted that privacy is a human right as well as an economic issue. They pointed out that the 1990s are likely to be a more focused, socially conscious decade, which see a shift in public policy toward social concerns. Countries are realizing that they must look beyond economic issues and address societal ones as well. In certain cases, and data protection may be one of them, what may have traditionally been "economic" issues may take on a far greater "social" emphasis. The human rights element may be that which in the end forces countries to act on the preservation of personal privacy.

The Workshop brought home the complexity of the privacy issue. Not only are we undergoing a rethinking of our definition of privacy, but we must do so in an international context, both economically and socially. Added to this is a broad range of interest groups, complex jurisdictional circumstances and increasingly sophisticated communications technologies. These complexities will mitigate against any simple solution to ensuring personal privacy and individual freedom. A range of options were explored during the Workshop, and it became abundantly clear that with balanced mix of regulation, technology solutions and codes of conduct we can address privacy and data protection concerns. Efforts by individual organizations like DOC, in cooperation with other relevant departments and agencies can make a positive contribution in this regard.

Increasing public concern for privacy, accompanied by the sophistication of communications technologies, can be expected to require strong privacy advocacy and leadership from government in the coming years. The unique position of the Department of Communications will allow it to play a pivotal role in ensuring that the social implications of communications technologies are considered in the development and introduction of new technologies and services.

## **INTRODUCTION**

A Strategic Planning Workshop on Privacy and Data Protection was held on December 5, 1991. The purpose of this Workshop was to explore emerging issues and their implications on the Department of Communications. Growing public concern over privacy infringement and international developments in data protection legislation present new and urgent challenges to DOC. Of particular concern to the Department are the strong linkages between the sophistication and use of communications technologies and apparent opportunities for privacy infringement.

Given global developments and the personal nature of the privacy issue, the Workshop was structured around three themes: Defining the Issues, International Influences and Developments and Responding to the Privacy Challenge. The structure of this report follows the agenda of the Workshop and summarizes the presentations of speakers. It also intends to give a flavour of the discussions which took place throughout the day. A copy of the agenda can be found in Appendix 2.

The Workshop Chairperson, Ms. Eileen Sarkar opened the session by providing participants with an overview of the Department of Communications' interest in privacy and its historical involvement and accomplishments in this area. She stressed the importance of cooperation if inroads are to be made in ensuring adequate privacy and data protection, particularly given international policy trends. Ms. Sarkar also stressed the need for a balanced approach and illustrated this by comparing the privacy issue to the environmental movement and copyright law. In both cases, the challenge has been to provide a balance between the needs of the "creator" and the "consumer".

## **KEYNOTE SPEAKER**

### **"Privacy is the Right to be left alone"**

The Workshop's keynote speech was given by David Flaherty, Professor of History, University of Western Ontario. Professor Flaherty forcefully reminded participants that privacy is a universal moral value which has several different dimensions:

- SOLITUDE - THE RIGHT NOT TO BE DISTURBED
- INTIMACY - THE RIGHT NOT TO MONITORED
- ANONYMITY - THE RIGHT NOT TO BE KNOWN
- RESERVE - THE RIGHT TO CONTROL ONES PERSONAL INFORMATION

In simplistic terms, privacy as originally defined by U.S. Justice Brandeis in 1890 and supported by Professor Flaherty, is the right to be left alone. Professor Flaherty went on to discuss public expectation and government's approach to protect the right to control one's personal information.

Human beings, Professor Flaherty pointed out, want to enjoy as much privacy as is possible, and participants were asked to reflect on their own needs as individuals as proof of this desire. With the increasing use and importance of information in today's economy, we are always leaving a "data trail" behind us as we go about our daily lives. Much of this occurs without our knowledge. Privacy has become something that we are unable to preserve on our own; we are rapidly losing control of our personal data and how it is used. Flaherty pointed to a number of public opinion polls and media reports which indicate the exponential growth in public concern over this lack of control.

Of particular interest to DOC is the consistency with which technology is referred to as the weapon of choice for the perpetrators of privacy invasions. The headline in the November 11, 1991, U.S. edition of TIME magazine featured the cover story, Individual Rights. Nowhere to Hide. Using computers, high tech gadgets and mountains of data, a growing army of snoops is waging an assault on America's privacy." The idea that technology may be behind this assault, both inhibits and provokes public response on the issue of privacy. People may either be prompted or reluctant to act because of the apparent impersonal nature of data collection and manipulation.

Flaherty suggested to participants that "fair information practices", such as outlined in the OECD Privacy Guidelines, should serve as a benchmark for determining what is an acceptable level of privacy protection. Under these guidelines, information collected must be:

- TIMELY AND RELEVANT
- COLLECTED LEGITIMATELY
- USED ONLY FOR THE PURPOSE INTENDED
- KEPT ONLY FOR A LIMITED PERIOD OF TIME

Professor Flaherty went on to outline the current privacy rights of Canadians. At this time, Canadians do not enjoy an explicit constitutional right to privacy. The Supreme Court, however, has through its interpretations of the Charter of Rights and Freedoms, established a reasonable expectation of privacy vis-à-vis the state. Justice Laforest, according to Flaherty, has been a strong supporter of privacy and his decisions in this regard should have earned him the title "Canada's Father of Privacy".

Canada's first Privacy legislation, was enacted in 1977 as part of the Human Rights Code, and constitutes a code of fair information practices. The Privacy Act followed in 1982. One of the problems with it, says Flaherty, is that it is not adequately enforced or implemented. The Province of Quebec has the strongest privacy provisions in Canada. The Quebec Civil Code makes specific reference to privacy and plans are underway now to extend its regulation into the private sector. Ontario, for its part, has taken steps recently to extend its privacy statute to include the municipalities. Nova Scotia and Saskatchewan are the only other provinces with privacy statutes.

Notably absent in Canada are sectoral data protection provisions which are commonly used in the United States. Canada's new Bank Act, which will have data protection provisions, is a rare exception.

Canada is a member of OECD, and adopted the 1981 OECD Privacy Guidelines in 1983. These guidelines are based on self regulation, but Canada to this point has had an abysmal record in terms of compliance. The private sector's failure to implement the OECD Guidelines and the limitations of the Privacy Act leave Canada in a very vulnerable position should the European Community's draft data protection directives be approved. These directives, which are the driving force internationally on data protection policy, would present serious trade barriers to Canadian companies. According to Flaherty, if Canada doesn't develop EC-type data protection laws, the flow of data between Europe and Canada could be virtually cut off.

In his closing remarks, Professor Flaherty stated that he believes that we are building surveillance societies of Orwellian proportions. The rush of innovations in information technology in the public and private sectors pose constant challenges to the preservation of personal privacy. He stressed the central importance of consciousness-raising at all levels of society and of making data protection as "anti-bureaucratic" as possible.

He outlined a number of measures which could be taken by government to address the public's right to privacy and to respond to international developments in data protection:

- PROMOTE GREATER COOPERATION AMONG DATA PROTECTION SPECIALISTS IN GOVERNMENT
- INCLUDE A PRIVACY PROTECTION PROVISION IN CANADA'S CONSTITUTION IN ORDER TO GUARANTEE A LEGAL RIGHT TO PRIVACY
- DEVELOP GOOD CANADIAN SURVEY DATA; WE CURRENTLY RELY ON U.S. DATA
- EXTEND CANADA'S CURRENT PRIVACY ACT TO INCLUDE FEDERALLY-REGULATED INDUSTRIES

### **DEFINING THE ISSUES**

The presentation by Professor Flaherty was followed by a stimulating and provocative panel discussion. The panel addressed the question as to what are the real privacy issues and explored the need for a balance between the conflicting demands of technological innovation and social values such as privacy. The interests of the consumer were aptly presented and defended by Mme. Madeleine Plamondon and Mr. Marc Rotenburg. Ms. Joanne DeLaurentiis and Mr. Brian Milton represented the views of industry.

The panel provoked such animated debate that the Discussion Groups which were to follow, were cancelled in favour of further discourse. The following is a summary of the presentations of each of the panellists and an overview of the questions which followed.

**MR. MARC ROTENBURG, EXECUTIVE DIRECTOR,  
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY**

"Privacy is about the auctioning of personal information"

Mr. Rotenburg's presentation focused on the issue of Caller ID. Mr. Rotenburg challenged the notion that in this instance privacy is about competing interests: the interest of the caller versus the interest of the recipient. What is at stake in the Caller ID issue, according to Rotenburg, is the loss of control of personal information. The argument that the recipient, whose privacy is intruded upon, has the major stake is, Rotenburg believes, an incomplete one. Previously, the caller had the option of whether or not to identify him or herself. That option has been taken away. The identity of the caller is now controlled by the telecom carrier, which can decide to reveal the information if the party subscribes to Caller ID: or it can withhold the information if the calling party subscribes to call blocking service. This, according to Mr. Rotenburg, amounts to the auctioning of personal information to the highest bidder. Mr. Rotenburg reinforced his point using the example of 1-800 numbers. He asked whether the merchant has the right to know the identity of the caller/buyer? Why should it be presumed to be acceptable when using a 1-800 number, while it would not be in a face-to-face transaction, where we have a choice?

In the case both with Caller ID and 1-800 numbers, the choice of deciding to whom one identifies oneself has been removed. The potential outcome of this type of loss of control was brought home in Mr. Rotenburg's example of the opposition by individual women and women's shelters to Caller ID services. He noted that it has been argued that the Caller ID service increases the possibility of harassment and violence in situations where it is important that the location of a female caller, and perhaps her children, not be disclosed.

**MR. BRIAN WILTON, DIRECTOR, GOVERNMENT RELATIONS, BELL CANADA**

"In the future, customer relations will be governed by the information involved rather than physical presence."

Mr. Milton argued that our definition of individual rights in the 1990s should bear little resemblance to that which we expected and perhaps received in the 1970s and 1980s.

According to Mr. Milton, in a market-oriented economic environment where competitive interest in information is very important, we must strike a balance between economic efficiency and privacy expectations. In certain instances, people must accept to pay the costs associated with options or solutions that are not necessarily "economically efficient". In Mr. Milton's words, "Outdated norms are not good for today's information world".

In commenting on Bell Canada's privacy priorities, Mr. Milton identified three areas of concern: tele-marketing, new services (ISDN), and data protection. In the area of telemarketing, Milton suggested that managers must become responsible for social as well as economic transactions. Bell Canada currently has in place a Code of Ethics, a set of management practices which acts as an employee guide in the proper use and care of customer information. He also indicated that he believes that a Code of Fair Information practices is imminent.

However, Mr. Milton also indicated that Bell Canada believes that there is a legitimate role for government regulation. He pointed out that Bell Canada only controls about 20% of the telemarketing area; telemarketing associations control about 40%, while the remaining 40% is totally unregulated. An adequate set of regulations would serve to govern the activities of the entire spectrum of participants in telemarketing.

**JOANNE DELAURENTIIS, VICE PRESIDENT, DOMESTIC BANKING AND PUBLIC AFFAIRS,  
CANADIAN BANKERS ASSOCIATION**

**"Data users and owners need to reach a consensus on how the principles of privacy should be enforced"**

According to Ms. DeLaurentiis, the Canadian banking industry is a strong advocate of self regulation and the use of voluntary codes. The Canadian Bankers Association released a model code in December 1990 and commercial banks have targeted the end of 1992 for implementation of similar codes. Codes, according to Ms. DeLaurentiis, can be both practical and educational. The position taken by the Canadian Bankers Association is that self regulation recognizes the need for sector specific understanding of issues and therefore provides for greater flexibility. Of primary importance is for stakeholders to reach a consensus on how privacy principles should be developed and enforced. The beneficiaries of this are both industry and customers alike.

With respect to the issue of determining ownership of personal data, Ms. DeLaurentiis questioned the need for explicit customer consent, particularly if the information remains within the organization which originally received the information. If the information was to be used and transferred to an outside organization, the situation would be different. She also suggested that marketing and regulatory regimes outside of Canada must be understood and accounted for on the domestic scene if Canadian companies are to remain competitive in a global economy.

**MADELEINE PLAMONDON, PRESIDENT AND DIRECTOR, CONSUMERS AID SERVICES**

"The time is past for discussion, we need regulation before there is a scandal."

Mme. Plamondon provided a consumers' perspective to the discussion of self regulation and industry codes. Regulation, according to Plamondon, is essential in order to redress situations where unreasonable demands or uses are made of personal information.

Mme. Plamondon argued that the codes of conduct being implemented by the Canadian banks are inadequate and self righteous. Codes, said Plamondon are only marketing tools - they look good, but like gruyere cheese, are full of holes!

In response to Ms. DeLaurentiis point on the virtues of self regulation by banks and their affiliates, Mme. Plamondon argued that the vertical integration within the industry means that an individual no longer has sufficient control as to how their personal information is managed and manipulated within the larger organization. We have moved she said beyond "big brother" to "a family...with sisters". She suggested that consumers will soon be taking matters into their own hands and developing model privacy codes, rather than waiting for either government or industry to act.

**Question Period**

The question period was dominated by discussion on the subject of Caller ID. As was pointed out by both the speakers and participants, Caller ID represents only the tip of the iceberg in terms of latent privacy issues which are likely to attract public attention. Rotenburg's opinion

was that Caller ID will pale in comparison to issues which arise as a result personal communications networks of the future.

Both Rotenburg and Plamondon made the point that secondary information disclosure is not a complex issue. It is about business crossing the line and trying to use information for purposes for which it was not intended - and without compensating the user. They argued that prior consent is the preferred option, rather than the opting out option as suggested by DeLaurentiis and Milton. Milton had made the point that secondary information disclosure, like Caller ID, is a matter of relative rights. De Laurentiis indicated that ownership of personal data was only an issue if it was used outside the originating institution. Only then would explicit customer consent be required.

One of the participants made reference to the attitude changes that we have seen with respect to the environmental movement and suggested that we may see a time when it will be unacceptable to make secondary use of information.

The question was also raised as to why technology developers do not spend more time and attention anticipating, and where possible mitigating, the negative impact of technologies and associated services on the individual. This point was also taken up in the presentation by Mr. Katz in the last panel session of the day.

#### Luncheon Speaker - Mr. Bruce Phillips, Privacy Commissioner

Mr. Phillips spoke to the participants about the need for a more proactive approach to privacy issues in Canada, particularly given the increase in public concern and the potential for infringement afforded by increasingly sophisticated technology. He pointed also to the need for a greater degree of cooperation among privacy advocates within government. Mr. Phillips indicated that while voluntary codes are perhaps the preferred option, it would appear that there is a legitimate regulatory role for government in some instances. He advised participants of his appearance before the Constitutional Review Committee on December 9, 1991 at which time he would be recommending that a right of privacy be enshrined in the Constitution.

With specific to DOC' role in privacy, Mr. Phillips encouraged the Department to take a leadership role in the telecommunications area. He specifically suggested that Telecommunications Privacy Principles be developed and modeled after those of the New

York State Public Service Commission. Mr. Phillips indicated that he would be very supportive of this type of initiative.

Panel Discussion - International Influences and Developments

Following lunch, a panel of international experts explored the resurgence of interest, particularly in Europe, in personal data protection and its implications on Canada from both a trade and social policy perspective. A common theme of the three presentations was that privacy is a human rights issue, and as such will continue to gain prominence in the coming years. Governments and industry will not be able to avoid an issue which, as the speakers pointed out, has ramifications of such enormous social and economic consequence.

MR. DAVID GOLDBERG, LECTURER, DEPARTMENT OF JURISPRUDENCE,  
UNIVERSITY OF GLASGOW

"Privacy is an international human rights issue, not a local concern".

Respect for privacy, said Goldberg, is an international norm. He noted that Canada is a signatory to a number of Human Rights Conventions in which the right to privacy is specifically addressed. Among these are the International Covenant on Political and Civil Rights and the Conference on Security and Cooperation in Europe.

Mr. Goldberg also spoke briefly about the proposed European data protection directives and the future he sees for them. The European Community is currently responding to the draft Directives. Approximately 300 amendments have been proposed and must be considered by the Legal Affairs Committee of the European Commission. The revised Directives will then be reviewed by the European Parliament and sent forward to the European Commission for further revision, probably in late 1992. He anticipates that a revised document will be issued by the European Parliament in mid-to-late 1993. Once ratified by the Commission, it could take another two years before it is ratified by member states.

The United Kingdom's response to the directives is, according to Goldberg, a wish that they (the directives) had never happened. In true British tradition, the main concern is with good handling practices". He illustrated this with the example of wayward puppies and their need for consistent, precise and concise directions!

**MR. HERBERT BURKERT, DIRECTOR OF RESEARCH, GMW,  
INFOW COLOGNE, GERMANY**

"In terms of privacy, the European Community is asking itself whether it wants a community of merchants or a community of citizens."

Mr. Burkert, like Goldberg, talked about privacy in terms of human rights. Human rights in the European context are regarded as elements of the social value system of societies. And this, he emphasized, was not just individual rights but also relations between individuals and groups. The European Economic Community may have been conceived originally as exclusively an economic organization, but it now is realizing that it must look beyond economic issues and address societal issues as well. Unlike Mr. Goldberg, who was somewhat pessimistic as to the likelihood of the directives receiving early ratification, Mr. Burkert was of the opinion that the European Court may become involved and force an earlier response.

Information is, Burkert reminded participants, not - commodity like any other. Our concept of commodities is changing - slaves, he pointed out, were perhaps the only other "commodity" that so radically challenged both our definition of a commodity and the economic order.

While different countries may handle information differently, Mr. Burkert does not believe that there should be disparities in rights between regions. You cannot, he said, ignore human rights when dealing with "nitty-gritty" issues.

**MR. EVAN HENDRICKS, EDITOR, PRIVACY TIMES, WASHINGTON, D.C.**

"Privacy is a sovereignty issue"

Mr. Hendricks began his presentation by asking participants whether they were aware that personal data on Canadian citizens is regularly shipped to other countries. Once out of Canada, he pointed out, our national laws have no power to deal with it. He gave the example of the Medical Information Bureau (MIB), which is located in Boston, Massachusetts. The MIB is an information bureau for insurance companies and is used regularly by a number of large Canadian insurance companies. He noted with some irony, that while there may be no system of informed consent, there is a very efficient system for moving data internationally.

While the United States is greatly concerned about the proposed European Data Directives, and in particular that part related to transborder dataflow, it has yet to take a constructive approach. That being the case, he suggested that a backlash is building in the European Community in response to the U.S. reaction, which could result in data cutoffs. The solution, says Hendricks, is a simple one - do the right thing and introduce adequate privacy policies and laws. Canada, he said, should stand aside from the U.S. on this issue and address rather than try to avoid and bypass the need for regulation.

Panel Discussion - Technology, Legislation, Codes of Conduct - What Are The Answers?

The third and final panel of the day focused on the options available to both government and industry to ensure that the privacy rights of individuals are protected. The speakers presented their views on the mix of technology, government regulation and self regulation available to address privacy infringement and data protection issues.

**MR. ROBERT GELLMAN, CHIEF COUNSEL, U.S. HOUSE OF REPRESENTATIVES  
SUBCOMMITTEE ON INFORMATION AND JUSTICE, WASHINGTON, D.C.**

"Privacy is not just a consumer concern, but a business one as well".

Mr. Gellman suggested that it is in the businessman's interest to resolve the privacy issue. As consumers begin to recognize the technological potential for privacy infringement, we will see the rejection of products and services which facilitate this infringement. Mr. Gellman gave the example of Lotus Marketplace, a database on 220 million households which was developed as a marketing tool but which was, as a result of consumer concern, never actually launched. Business must concern itself with the public's concern for the misuse of information and establish clear guidelines for the use to which legitimately collected information will be put. Regulations, said Gellman, can avoid dilemmas. He illustrated this with the following scenario: a woman is raped in a grocery store parking lot, and under police questioning, recalls seeing a grocery store bag in the car and the specific items it contained. The owner of that store is faced with two possible newspaper headlines: "Store owner uses customer information profile to track individual" or "Store owner refuses to cooperate with police". Neither situation is enviable. Regulations which governed the use of personal data would avoid this dilemma.

Gellman pointed out that the United States has adopted a piecemeal approach to privacy and data protection which has resulted in less than satisfactory results. The fact that Canada has a Privacy Commissioner, does according to Gellman, put us in an advantageous position - at least in theory. What we must ensure is that adequate power and resources accompany the office.

**MR. JIM KATZ - BELLCORE**

"Technologies are privacy neutral, but the way they are used may not be."

Mr. Katz began his presentation by showing a short video of a new technology which has been developed by Bellcore called, "Cruiser". Cruiser uses video and broadband technologies to visually and electronically network individuals in a work setting. The user would have a Cruiser terminal on their desk as well as video cameras at his/her desk and door. Using the system's video capabilities, the user can "cruise" the building looking for colleagues that he/she wishes to consult with on a particular subject. Once the appropriate individual(s) is located, the relevant documentation could be presented using the desk mounted video camera and transmitted electronically for comments and discussion between the individuals. While this technology offers exciting possibilities for networking, problem-solving and joint research, as well as the obvious benefits for the physically-handicapped, it has negative connotations also. The spectre of "big brother" looms whenever one suggests the monitoring of the comings and goings of individuals.

Mr. Katz believes that one must recognize and accept that the privacy implications of a particular technology or service can not always be known beforehand. He does, however, see the need for a set of explicit privacy policies to guide the development and introduction of new technologies. These guidelines would, he explained, serve a function similar to that of fire codes.

**MR. PHILIP PALMER, GENERAL COUNSEL, LEGAL SERVICES,  
DEPARTMENT OF COMMUNICATIONS**

"The 1990s will be a very different decade. It will be a more focused and socially conscious decade."

Mr. Palmer, in his opening remarks, concurred with Mr. Flaherty's observation that the Canadian courts have created the right to privacy. He however was not as supportive of a constitutional approach to privacy. The downside of a Constitutional amendment to enshrine a right to privacy would be to increase the ability of private interest groups to capture the public agenda. A balanced approach to public interest may not be best served in the Courts.

Mr. Palmer was supportive of efforts to extend the current privacy legislation to include federally-regulated industries. The sectoral approach taken in the United States would, he believes, not fly in Canada given the general lack of awareness within industry of the economic and policy implications of privacy. Either way, a joint effort of federal and provincial governments will be required, given that from a jurisdictional perspective, the greatest mass of privacy activity rests with the provinces. Without cooperation and harmonization, we are likely to see an uneven playing field created.

Regulation is another alternative. Codes of conduct could be imposed by regulatory bodies such as the CRTC, or industry could choose to regulate itself. The Canadian Bankers Association has adopted the latter approach, but as Mr. Palmer pointed out, self regulation is generally only successful where there is an independent "watchdog" in place.

The 1990s, according to Palmer, will be a very different decade from that which we have experienced previously. We will see a more focused, socially conscious decade following on the demise of the Cold War and the madness of the Gulf War, which was won with high power weaponry and information. We should expect to see a shift in public focus to social concerns and with it will come ever increasing concern with the commodification of personal information. According to Mr. Palmer, that will be the key privacy issue of the 1990s and it represents a new and real danger to individual freedom.

**CHAIRPERSON'S CLOSING REMARKS**

The Chairperson's closing comments emphasized the point that privacy is everyone's concern. Ms. Sarkar reminded participants that we are likely to experience an increase in public expectation for government leadership in the area of privacy. This will, she pointed out, require a delicate balance of what may prove to be competing interests. Our success in dealing with this issue will depend greatly on our commitment and ability to work together. We can all benefit from a partnership which supports and encourages dialogue and cooperation.

Ms. Sarkar noted that DOC has the unique responsibility of ensuring that Canadians have access to an efficient and effective telecommunications system, while at the same time ensuring that the social implications of the technologies are understood and addressed. This responsibility and expertise will place DOC at the centre of the telecommunications privacy issue and will require an open-minded and yet vigilant approach to policy-making.

PRIVACY AND DATA PROTECTION WORKSHOP

DECEMBER 5, 1991

SUSSEX ROOM, GOVERNMENT CONFERENCE CENTRE

SADM

Sean Berrigan, DPG, DGSP  
Raymond Lepage, DSP, DGSP  
Sharon Jeannotte, DSP, DGSP  
Brenda Patterson, DSP, DGSP  
David Waung, DSP, DGSP  
Suzanne Loranger, DSP, DGSP  
Claude Hébert, DSP, DGSP  
Suzy Beauregard, DSP, DGSP

Ninon Charlebois, DGIS

Stephanie Perrin, DGIR  
Tamara Andruszkiewicz, DGIR  
Bob Tritt, DGIR  
Leonard Hiho, DGIR  
Charles Vallerand, DGIR

Dave Dawson, DGRO

Heather Black, DLS

ADMRS

Mary Frances Laughton, DTA, DGCP  
Helen McDonald, DPP, DGCP  
Randy Zadra, DMS, DGCP  
Lewis Scott, DPM, DGCP  
Arthur Cordell, DGCP  
Bill Graham, DPP, DGCP  
Alister Pederson, DPM, DGCP  
Frank Symons, DMS, DGCP  
Bob Baser, DMS, DGCP  
Susan Baldwin, DTP  
Winnie Pietrykowski, DPP  
Prabir Neogi, DPP, DGCP  
Luc Fournier, DPP, DGCP

Nur Serinken, DRL, DGRC

George Zurakowski, DBC-P, DGBR  
Ralph Zeitoun, DBC-E, DGBR

Ron Morley, DBR, DGBT

Ina Bischof, DRP, DGRR  
Jan Skóra, DRP, DGRR

Maria Morin, DDE, GTA

### MINO

Kevin Lamarque  
Vaughn Lantz

### ADMCP

Jamie Hum, DGNM  
Thérèse Rivet, DGNM  
Richard Simpson, DGNM

Maurice Eastabrooks, DGTP  
Janet Witt, DGTP  
Vic Banning, DGTP  
Doug McEwen, DGTP  
Parke Davis, DGTP  
Alan Hamilton, DGTP  
Susane Latrémouille, DGTP  
Serge Presseau, DGTP  
Michael Helm, DGTP  
David Warnes, DGTP

### ADMCM

Susan Mongrain, ATIP

### ADMAH

Barbara Rottenburg, CHIN

## **SMAQ**

Judy Marsh, APU  
Susan Gillies, CWARC

## **REGIONS**

Ivan Cartwright, Pacific Region

## **EXTERNAL**

Anna Markapoulos, Finance  
Dan Roseman, External Affairs  
Robert Hayward, Treasury Board  
Mary Champoux, Treasury Board  
Mary Anne Stevens, Treasury Board  
Ken Katz, CRTC  
Barry Bondar, Regulatory Reform  
Susan Scott, Office of the Privacy Commissioner  
Louis Alberti, Office of the Privacy Commissioner  
Brian Foran, Office of the Privacy Commissioner  
Ann Goldsmith, Office of the Privacy Commissioner  
Julien Delisle, Office of the Privacy Commissioner  
Sally Jackson, Office of the Privacy Commissioner  
Jerry Montigny, Office of the Privacy Commissioner  
Karen Adams, Canadian Library Association  
Lloyd Younger, Justice  
Andrea Neil, Justice  
Peter Robinson, Consultant  
Tom Riley, Consultant  
Robert Parent, MCQ  
Doreen Guthrie, Consumers Association of Canada

## **SPEAKERS**

Eileen Sarkar, Director General, Strategy and Plans, DOC  
David Flaherty, Professor of History, University of Western Ontario  
David McKendry, Price Waterhouse  
Madeleine Plamondon, President, Consumer Aid Services, Shawinigan  
Marc Rotenburg, Executive Director, Computer Professionals for Social Responsibility, Washington, DC  
Joanne DeLaurentiis, Vice-President, Domestic Banking and Public Affairs, Canadian Bankers Association

Brian Milton, Director, Government Relations, Bell Canada  
Bruce Phillips, Privacy Commissioner  
Herbert Burkert, Director of Research, GMW, INFOW Cologne, Germany  
Evan Hendricks, Editor, Privacy Times, Washington, DC  
David Goldberg, Lecturer, Department of Jurisprudence, University of Glasgow  
Elisabeth Châtillon, Director General, International Relations, DOC  
Philip Palmer, General Counsel, Legal Services, DOC  
James Katz, Bellcore  
Robert Gellman, Chief Counsel, US House of Representatives, Subcommittee on Information  
and Justice, Washington, DC

**PRIVACY AND DATA PROTECTION WORKSHOP****DECEMBER 5, 1991****SUSSEX ROOM, GOVERNMENT CONFERENCE CENTRE  
2 RIDEAU STREET, OTTAWA**

9:00 - 9:15

**Welcoming Remarks by Chairperson, Eileen Sarkar,  
DGSP**

Current international developments in data protection legislation in response to privacy implications of new telecommunications services and growing public concern over privacy infringement could present new and urgent challenges to DOC. The growing importance of information as a valuable and critical commodity may be adding urgency to the problem. Canadians will be expecting strong privacy advocacy and leadership from government in the next few years. What role should DOC play to ensure that our social and economic concerns are properly balanced?

9:15 - 9:45

**Keynote Speaker - David Flaherty, Professor of History, University  
of Western Ontario**

David Flaherty, is an internationally recognized expert on privacy issues, and was the resource specialist for the Parliamentary Committee on Justices and the Solicitor General which reviewed Canada's Access and Privacy Legislation in 1986. Mr. Flaherty will describe the various social, economic, political and technical forces that are influencing, and at times creating, issues and trends in privacy and data protection. He will also pose for us, some of the challenges that government will be expected to address and the pitfalls if we fail to do so.

9:45 - 10:00

**Questions**

10:00 - 10:15

**COFFEE**

10:15 - 11:15

**Panel Discussion - Defining the Issues**

We have invited representatives from two critical information industries, the telecom carriers and the banks, to debate with consumer advocates as to what the real privacy issues are, and how they should be approached.

We are seeing increasing demands for privacy protection in the development of information products and services, particularly given their potential for infringement on an individual's right to privacy. The panellists will explore the need to provide a balance between the conflicting demands of technological innovation and social values such as privacy.

**Moderator - David McKendry, Price Waterhouse**

Ms. Madeleine Plamondon, President and Director,  
Consumer Aid Services / Service d'aide au Consommateur, Shawinigan

Mr. Marc Rotenburg, Executive Director, Computer Professionals for Social Responsibility, Washington, D.C.

Ms. Joanne DeLaurentiis, V.P., Domestic Banking and Public Affairs -  
Canadian Bankers Association

Mr. Brian Milton, Director Government Relations, Bell Canada

11:15-12:30

#### **Discussion Groups**

Facilitators will lead participants in a discussion of the policy implications for DOC of emerging privacy and data protection issues. Should DOC have a carefully developed and strongly advocated position on privacy issues related to, for example, the operation of integrated services digital networks and public digital mobile networks? What privacy safeguards should govern new services such as fax, call forwarding and call recording? And what about new cable services - inter-active cable, pay-per-view and the merging communications technologies in pursuit of the wired city? How do we address these policy issues effectively as public servants?

12:30 - 1:15

LUNCH

1:15 - 1:30

**Coffee and Dessert - Guest Speaker - Mr. Bruce Phillips, Privacy Commissioner**

1:30 - 2:00

**Reports from Discussion Groups**

2:00 - 2:45

**Panel Discussion : International Influences and Developments**

We are seeing a resurgence of interest in European countries in personal data protection issues, particularly with the approach of economic union in 1992. What exactly is proposed? Are there cultural differences between European and North American expectations of privacy that we will never be able to rationalize? What are the potential repercussions on trade with North America? What will the impact of these changes have on the design and operation of information networks and services? Are we being left behind?

**Moderator:** Ms. Stephanie Perrin, DOC

Mr. Herbert Burkert, Director of Research, GMW, INFOW Cologne, Germany

Mr. Evan Hendricks, Editor, Privacy Times, Washington, D.C.

Mr. David Goldberg, Lecturer, Department of Jurisprudence, University of Glasgow

2:45 - 3:00

COFFEE

3:00 - 4:00

**Panel Discussion - Technology, Legislation, Codes of Conduct - What are the Answers?**

Whether we are talking about privacy infringement or data protection, we can be certain that there is going to be pressure put on government to protect the rights of the individual, as well as to ensure that Canadian companies can continue to sell their products and services internationally and undertake joint ventures. What is the right mix of technology, government regulation, self regulation? And who is responsible for what? What leadership role(s) should DOC be taking?

**Moderator:** Ms. Elizabeth Châtillon, DOC

Mr. Philip Palmer, General Counsel, Legal Services, DOC

Mr. James Katz, Bellcore

Mr. Robert Gellman, Chief Counsel, U.S. House of Representatives Subcommittee on Information and Justice, Washington, D.C.

4:00 - 4:15

**Chairperson's CLOSING COMMENTS**



## PRIVACY THE ISSUE

PREPARED BY THE DOC  
PRIVACY WORKING GROUP  
JANUARY 1992



---

## PRIVACY - THE ISSUE

### 1.0 THE PRIVACY ISSUE

Information technology, with its potential for instantaneous transactions and its multi-jurisdictional characteristics, presents new and difficult problems for policy makers, technology developers and technology users. Privacy is one of those difficult problems. Privacy concerns are focused mainly on data protection, that is, matters related to security and use of information collected. There is however, increasing public awareness of privacy issues and insistence that information be used only for the purpose for which it was collected, and that it not be used for another purpose without the relevant individual's consent. Current economic trends where information is recognized as a valuable commodity in marketing is adding considerable urgency to the problem.

Current international developments in data protection, broad privacy implications of new telecommunications services and the growing public concern over privacy infringement present a new and urgent challenge to DOC. The issues these challenges present are as follows:

- a) *Increased public concern over telecommunications privacy*
- b) *Importance of privacy protection legislation on international trade*

### 1.1 Increased Public Concern Over Telecommunications Privacy

Privacy concerns are expected to increase as people realize the potential for intrusion into their lives and that information about them is being bought, sold and exchanged by both the private sector and government. The conflicting demands of technological innovation and social values are ones with which DOC, as the proponent of communications and information technologies, must concern itself.

### ADVANCED TELECOMMUNICATIONS SERVICES

Consumers are demanding privacy protection in the development and use of information products and services. The loss of anonymity associated with the use of telecom services such as Caller ID and 1-800 numbers has raised significant interest and concern in the private sector. So much so, that privacy has emerged as a critical factor in determining the rise or fall of certain products. Given the potential for developments in communications technologies to affect privacy expectations, the issue of whether or not privacy should be a consideration in approving the introduction of new telecommunication services must now be addressed.

### CELLULAR PHONES AND PRIVACY

The public continues to be concerned with the potential interception of private cellular radio communications and there have been some calls for legislation to make the interception of cellular radio telephone calls an illegal offence. While technological solutions may alleviate part of the threat, the feasibility of prohibiting the unauthorized disclosure of intercepted conversations must also be addressed.

As mentioned previously, increasing public attention is being given to matters associated with personal privacy. To illustrate these developments, the following information/cases in point are provided:

- ◆ The Department of Communications receives about 5 letters a month complaining about the privacy implications of Caller Display or Caller ID. As the service is introduced across Canada, letters come in from the areas affected. Caller ID was introduced first in Ottawa and Quebec City. It is currently being introduced in Montreal, Toronto and Vancouver. The CRTC receives more complaints but the exact number is unknown. The complaints are about: loss of privacy, threats to women living in shelters for battered women, the price of privacy (to block outgoing calls the call must be placed through an operator at 75 cents per call), inability to return calls by medical doctors, social workers, psychologists, etc., when the wish is to keep the home phone private, fear that people will not call help lines (suicide prevention, crisis intervention, etc.) since their number is displayed and can be easily matched to a name;

- ◆ The Privacy Commissioner of Canada has shown concern with information technology in general and telephone technology in particular. The annual report of 1990-91 reviews among other matters, data matching by different government departments, the projected use of smart cards by Employment and Immigration for unemployment benefits, and the possible misuse of an automated voice response enquiry system at Employment and Immigration (using someone else's SIN number it was possible to enter the EIC computer system and get information about that person). Although its mandate covers federal government departments, the annual report of the Privacy Commissioner contains a general discussion of privacy issues that affect Canadians. The most recent report also commented on privacy infringement in the use of cellular telephones; "also needed is for Parliament to restore privacy to telephone communications in Canada, now eroding with the spread of cellular telephones. Cellular communications can and are being intercepted by easily available monitoring equipment." The report goes on to suggest restrictions on the sale of monitoring equipment. The 1991-1992 Report of the Privacy Commission to be released in June, 1992 is expected to have a section on the privacy implications of telephone caller ID;
- ◆ The Consumers Fight Back Association (CFBA) has asked the Canadian Federal Court of Appeal to review the CRTC's decision allowing Bell Canada to offer Caller ID with operator-assisted blocking at 75 cents. In its application for leave to appeal, the CFBA argued that Call Display or Caller ID may violate laws governing the interception of private communications (wiretap laws) as well as the Charter of Rights and Freedoms. "The electronic display of the calling party's telephone number is clearly within the definition of 'telecommunication'. It is also a communication which the calling party reasonably expects will not be intercepted by anyone, including the receiving party, without the calling party's consent. Electronic display of the calling number is therefore a 'private communication' for the purposes of the Criminal Code." CFBA further alleges that the 75 cent fee per call block "... puts a price on the fundamental human value of the privacy of personal information. The charge also threatens to make privacy a privilege of the wealthy." (Source: Telecommunications Reports, April 22, 1991);
- ◆ In a 1982 survey by the Government of Ontario Task Force on Microelectronics, respondents were given a list of 13 issues related to microelectronics and were asked to indicate the five most important. The issue

chosen most often (by 63 percent of respondents) was privacy and confidentiality of personal information. The next three most important issues were accuracy of billing, control of information, and job security. In a more recent but more limited survey conducted in 1983 about interactive cable systems, concern for privacy scored very high. The survey was conducted in 210 homes in London, Ontario. Personal privacy was rated as more important than stopping the spread of nuclear weapons. The right to privacy was rated as more important than that of freedom of speech, freedom of the press and sexual equality. Moreover, fully 68 percent of the people interviewed believed Canadians had less privacy in 1983 than in 1973. Sixty-two percent indicated that they were concerned about threats to their personal privacy.

- ◆ The State of Pennsylvania ruled that Caller ID violates state wiretap laws and constitutional privacy in the United States;
- ◆ A 1988 survey found that nearly three out of ten Americans think about telephones when they think about privacy invasion. The question was asked: "Please give me an example of what you would consider an invasion of your personal privacy?" The telephone-related responses had to do with concern about telephone tapping, telemarketing, obscene phone calls, wrong numbers. (The other possible categories for privacy invasion were physical intrusion, questions about the person's emotional state or religion, misuse of personal information, limits to personal actions). (Source: Telecommunications Policy, April 1991 "Public Concern Over Privacy: The Phone Is The Focus";
- ◆ A Louis Harris poll conducted for Equifax in 1990 contains the following:
  - people were asked the following: "A new telephone service 'Caller ID', is available in some states. People with this service will be able to see the telephone number of the person calling them. Do you think telephone companies should be allowed to sell this service to people who want to buy it, or not?" 55 percent said yes and 43 percent said no (2 percent undecided).
  - presented with the options of making Caller ID freely available, making Caller ID available but regulated, or prohibiting Caller ID entirely, the American public preferred to make Caller ID available only if regulated. A significant minority (25 percent) indicated that Caller ID should be forbidden by law.

- nearly four Americans in five (79 percent) expressed general concern about threats to personal privacy. This is up from 77 percent in 1983 and up from 64 percent in 1978.
- three in ten Americans today, compared with only 14 percent in 1978, have decided not to apply for a job, credit, or insurance because they did not want to provide certain kinds of information about themselves.
- a majority of the American public (55 percent) favours protecting consumer privacy by using the present system (31 percent) or setting up a non-regulatory board (24 percent). A strong minority (41 percent) believe a regulatory privacy commission is needed.

## 1.2 Importance of Privacy Protection Legislation on International Trade

Most member countries of the European Community (EC) have data protection controls governing both the public and private sectors. Efforts are now underway to strengthen and harmonize the controls in preparation of a single European market in 1992.

In July 1990, the EC issued two draft directives governing the protection of personal data (one on data protection, the other on the telecom - ISDN data environment). The directives are designed to:

- ◆ establish a uniform, high level of privacy protection in both the public and the private sectors;
- ◆ remove barriers to the free flow of personal data among member companies.

If adopted, these directives would take effect in all EC member countries on January 1, 1993.

These directives have serious implications for Canadian companies doing business with Europe. Canada's current data protection standards do not provide sufficient data protection guarantees to meet the stringent guidelines proposed by the European Community. Without comparable data protection or laws governing its public and private sectors, Canada will be severely restricted in trade matters. In effect, European data protection laws would form a "data bloc"; if adopted, these standards would act as a strong and very effective non-tariff barrier to those countries unable to provide a comparable level of data protection. Some critics have argued that implementation of such a standard would allow the EC to control much of the world's information flow. Given current Canadian law, it is unlikely that the private sector could prove that it adequately protects personal data.

This "Eurocentric" approach is worrisome for North American companies. In the U.S., private industry appears to have recognized the potential impact of these proposed directives and is discussing with its government the need for similar privacy regulations to govern both the public and private sectors. Like Canada, current U.S. privacy legislation covers only the public sector. A bill was recently introduced in the U.S. legislature which updates the Privacy Act of 1974. That bill calls for the establishment of a federal data protection agency.

With the globalization of markets and Europe 1992 just around the corner, Canadian firms risk being at a competitive disadvantage. Given the critical importance of information in today's global economy, steps must be taken to ensure that the effects of these proposed directives do not restrict the competitiveness of Canadian industry. Canadian business does not appear to be as aware of, and/or concerned with, the potential implications of a single EC privacy standard. The absence of any substantive private, and perhaps public initiative, has resulted in a situation where the world's data protectors no longer regard Canada as a safe jurisdiction for data transfer. Canada's Privacy Commissioner has recommended that Parliament amend the Privacy Act to require federally-regulated private sector companies to "develop, file and implement privacy codes based on the internationally accepted principles established in the OECD guidelines".

## 2.0 PRIVACY LEGISLATION IN CANADA

### CANADA'S PRIVACY ACT

The declared purpose of Canada's Privacy Act enacted in 1982, was to protect the privacy of individuals with respect to personal information held by government institutions. More specifically, it provides Canadians with access to their personal information held by the federal government, places limitations on those who may see the information, and grants individuals some control over the government's collection and use of the information. But neither Crown corporations nor the private sector are covered by existing legislation. Since Canada adheres to the OECD guidelines on data protection, the private sector has been encouraged to develop their own codes based on the guidelines. Voluntary compliance on the part of the private sector, however, has proven disappointing.

The Act is structured in a manner similar to legislation in other countries. It gives a set of principles for the fair treatment of personal data, subject to certain exemptions - those related to individual access and those related to the disclosure of information to other organizations. In the 1970's, the possibility of developing an international convention on data protection was growing as both European and North American countries encountered problems of transborder data flows. The difficulty in protecting privacy rights in different legal jurisdictions led both the Council of Europe and the OECD respectively, to adopt a common standard of data protection legislation in 1980.

The guidelines developed by the Council of Europe and the OECD, the latter of which Canada adhered to in 1983, find expression in the Canadian Privacy Act. Sometimes referred to as a "code of fair information guidelines", the OECD guidelines present eight "basic principles of national application" as a model data protection statute. These guidelines include: the limitation of collection information, data quality, purpose, specification of information, use limitation, security safeguards, openness or transparency for the data subject, individual participation and finally, accountability of the data keeper. The OECD encouraged countries to adopt the guidelines and urged companies to comply voluntarily with the principles. As mentioned however, Canada has done little to promote company acceptance.

### PRIVACY LEGISLATION IN QUEBEC

On October 8 1991, a Quebec parliamentary commission on privacy protection - Commission parlementaire des institutions - held public hearings to examine privacy protection in the province's private sector. The Commission mandate is to :

- ♦ examine briefs submitted by the general public (private citizens and organizations) on the implications of the collection of personal information and the creation of data banks;
- ♦ study ideas on how to complement the provisions on privacy found in Bill 125 - The Civil Code of Quebec;
- ♦ examine recommendations on the protection of personal information submitted by the provincial government's interministerial committee on privacy protection entitled Vie privée: zone à accès restreint of April 1989.

According to Quebec's Privacy Commissioner Paul-André Comeau, the Parliamentary Commission was initiated in response to two key developments: 1) provisions in the new provincial civil code which will take effect January 1994, include pertinent sections related to privacy in the public and private sectors; and 2) the European Community's draft directives on privacy and data protection.

### BELL CANADA

Discussions with Bell Canada officials indicate that Bell has already drafted a set of guidelines which would act as a standard against which new advanced telecommunications services would be measured. However, these guidelines have not been formally adopted. Among the considerations is a concern that, adopted unilaterally by Bell, the guidelines may become a "burden" which could affect the company's competitive position.

### CANADIAN STANDARDS ASSOCIATION (CSA) INITIATIVE

In recent years, the CSA has embarked on a number of standards-setting activities in less tangible safety areas. They are currently considering developing a draft standard for privacy and data protection which they in turn would promulgate to business.

Organizations such as Pizza Pizza or Black's Cameras, which hold central databases containing information about their customers' buying habits along with credit information, would be eligible for a CSA seal of approval if they met the standards of the privacy code.

DOC works with the CSA in many areas having to do with the certification of equipment and network protocols. Their privacy standards idea, while embryonic at this stage, has considerable appeal given that CSA is an independent, highly respected and well known organization. CSA is looking for \$20,000 to fund a study which would develop a draft protocol. Price-Waterhouse's division of Consumer Affairs Consulting, which originally suggested the concept to the CSA, is the proposed contractor. Preliminary discussions have been held between CSA and DOC officials.

### 3.0 DOC AND PRIVACY

Through its technology development and international activities, DOC has continued to keep abreast of developments in privacy policies and regulations, but has not participated in or undertaken any significant privacy-related initiatives. It has been suggested that since the 1980's, DOC has focused its attentions on technology promotion and implementation and perhaps has not given sufficient attention to public good issues such as privacy. The broad privacy implications of communications, both from a social and an economic development perspective, make it imperative that DOC demonstrate leadership in the domain of privacy, telecommunications and data protection. To accomplish this, the following strategic initiatives could be considered:

1. *Privacy in Telecommunications Principles;*
2. *Extension of Canada's Privacy Act to federally - regulated industries.*

These particular initiatives have the potential to "re-involve" the Department in an issue which has both social and economic consequences for Canadians. And, equally important, privacy in telecommunications is an issue for which DOC has a clear jurisdictional responsibility. The proposed initiatives are not tied to one another. The Extension of the Privacy Act is a longer term initiative which would require the co-operation of other departments and agencies. The Principles initiative, on the other hand, is shorter-term and within DOC's mandate.

The Department, through its telecommunications policy mandate, must concern itself not only with the development of policies that enhance the provision of efficient and effective telecommunications services and facilities, but also with ensuring that the social implications of advanced telecommunications services are understood and addressed. In addition to its legislative and regulatory responsibilities for telecom policy, DOC has a responsibility to increase the country's scientific and technical expertise, coupled with facilitating the development, implementation and adoption of communications technologies, systems and services. A critical input into all of this, is an appreciation of the implications of new communications systems and services on the well-being of the individual and the country as a whole.

### 3.1 PRIVACY PRINCIPLES

The first proposed initiative, the Privacy Principles would in effect provide guidance and a framework for deciding privacy-related issues and would underline the fact that privacy should be considered an issue when deliberating on the introduction of new telecommunications services. The Principles would also serve as a signal to both industry and the general public on the need for greater emphasis on educating users about new services and privacy-related options.

There are a variety of mechanisms open to DOC for developing and implementing a set of privacy principles in the context of the new telecommunications environment in Canada. The overall process can be broken down into two phases or sets of activities. The first would involve the development of a set of principles on telecommunications privacy. This could involve considerable public consultation and participation. The second would relate to the implementation of the principles developed in the first phase. This would, depending on the option chosen, involve the Minister of Communications to varying degrees.

### 3.2 EXTENSION OF PRIVACY ACT TO FEDERALLY-REGULATED PRIVATE SECTOR

The second proposed initiative, Extension of Canada's Privacy Act to the Federally-regulated Private Sector, is longer-term in nature. As has been stated earlier, Canada's private sector is not governed by any privacy legislation. While Canada was instrumental in drafting and promulgating the OECD Guidelines for Data Protection in

1980, there has been little interest by Canadian industry to comply with these guidelines. It should also be noted that the EC guidelines currently being proposed are far more stringent than those issued by the OECD in 1980.

It would appear that Canadian industry is relatively uninformed as to the developments and implications of the EC directives. At a recent DOC seminar, Alan Leadbeater, former Executive Director, Office of the Privacy Commissioner, noted that "street level knowledge is almost zero... (and) I can't help but wonder whether it's any higher in the boardrooms of the nation." It would certainly appear that Canadian industry could benefit from some strong leadership in the next few years.

There are many departments and agencies implicated in data protection, including Justice, External Affairs, Finance, Treasury Board, Consumer and Corporate Affairs, the Office of the Privacy Commissioner and DOC. DOC is the department responsible for monitoring the EC telecom directives, as well as other OECD initiatives. As such, **DOC must continue to play the central role in co-ordinating a Canadian response to the directives and to encourage within Canada an awareness of the possible "data bloc" implications.**

Due to the complexity of the problem, and the number of parties involved in the issue (both public and private), it would be unrealistic to expect any short-term success with respect to extending the Privacy Act to federally-regulated private corporations. However, **DOC is committed to addressing the data protection "void" within Canada and is willing to partner with the relevant parties.**

Federally-regulated private companies which would be affected by the extension would be corporations involved in banking, pipelines, navigation and shipping, telecommunications, broadcasting, transportation (including interprovincial railways, interprovincial ferries, airlines). It is worth noting that the banking industry in Canada has been active in the data protection field for some time (going back to the 1970's with Roland Frazee of the Royal Bank) and the Canadian Bankers Association has developed a model privacy code for adoption by its members.

---

#### 4.0 CURRENT PRIVACY RELATED ACTIVITIES UNDERWAY IN DOC

##### 4.1 Policy Planning

A departmental working group chaired by DGSP has been established to examine the emerging privacy issues as they relate to DOC's mandate. The Working Group includes representatives from corporate and sector strategic planning, telecom policy, international relations and legal services. In May, 1991 DGSP held an information seminar on "Privacy and Data Protection in the 1990's" which was well attended by departmental staff. This was followed up by a one day Strategic Planning Workshop on December 5, 1991. The workshop featured Canadian and international privacy experts and considered the various forces and developments which are influencing issues and trends in privacy and data protection.

The Telecommunications Policy Branch (DGTP) is currently developing a policy statement on privacy in telecommunications which will include privacy principles. The Department's Privacy Working Group will be assisting in these efforts.

The Communications Development and Planning Branch (DGCP) is preparing a discussion paper concerning the introduction of a personal numbering plan associated with a personal communications device. The paper will address the question of privacy and how it can be protected in a personal communications environment.

##### 4.2 Research

The Communications Technology Research Branch (DGRC) has undertaken research in the area of security for voice and data transmitted over radio systems. A security system using public key techniques for E-mail and FAX has been developed for a marine radio data system. The technology was recently transferred to Ultimateast, St. John's, Newfoundland where it will undergo further evaluation and development.

Research into providing security for digital cellular radios on hold until the specifications for the new digital cellular is resolved.

[illegible]

Canada