PRIVACY AND SECURITY OF DATA BANKS

R.J. Friesen
Research Consultant, Security Systems Branch,
"P" Directorate, RCMP, Ottawa

This is a cursory look at the concept of personal privacy and its relationship to security in automated information systems.

Personal privacy and security of information are both subjects which, in themselves, could be discussed in great length and not be covered completely. In fact, the concerns for privacy are still changing and developing. In Canada, legislation is now before the House of Commons dealing with discrimination and the protection of personal privacy respecting personal information in federal information systems and this will have far-reaching significance on how we will look at the protection of privacy respecting personal information and its uses.

The concern for personal privacy and automated information systems began about 1965 when the Social Science Research Council in the USA proposed a central repository for all socio-economic data. Some apprehension arose that this would result in dossiers being created on everyone with great risk of misuse and privacy violation[1].

Some of the first legislative proposals in the USA in the early 1970's were directed toward computerized information banks, where the threat was thought to be, rather than manually operated systems. Today, however, there are good indications that privacy protection could be made easier if information was stored in a central repository where it would be easier to control and protect and where it might provide an individual with easier access to information about himself. This is somewhat of a reversal of the earlier thinking and is perhaps an illustration of the changing and developing views of how privacy, respecting personal information, might be protected.

Because of the concern for security of information that is now being processed in automated systems, security is also being looked at differently and is becoming sophisticated.

---

1 "Concepts for Privacy of Federal Records", Robert H. Courtney. The Social Science Research Council (Ruggles, 1965)

The concepts of personal privacy and information security, and the relationship between the two, continue to evolve as our understanding of both progresses.

There is a story about a hairy prehistoric man standing near the edge of a forest early one evening. The mist shrouded the horizon as the moon began to rise above the trees. The prehistoric man looked at it, seemingly not too far above the tree branches, and decided it would be a good idea if he were to bring it down, examine it closely and find out what it was. So he climbed up the tallest tree but soon found he was still a long way from being able to take the moon into his grasp. He then looked down to the ground and observed that although he hadn't yet reached his objective, his project was at least off the ground[2].

This is not unlike our present situation with respect to our understanding and analysis of personal privacy. We are making progress but we have a long way to go before we know what personal privacy really is and what the long-term solution will be in protecting it, if it can be protected at all.

Attempts have been made to define personal privacy, and then to draft legislation that would prevent any conduct that would violate that definition of privacy. This approach fails because of our failure to be able to define personal privacy. A person may want to protect certain information about himself from exposure at one time and want the same data exposed at another time. At one time in a woman's life, for example, she would object strongly to her age being made known. Later, when she comes near to qualifying for old age pension, she may become quite happy to reveal her age.

A person may feel that revealing certain critical parts of his personal file would violate his personal privacy, but at the same time he would be quite happy to see some of the good things made known.

What is private to a person at one time may be something he is anxious to reveal at some other time and vice versa. That sort of thing varies from person to person from one time to another. There is no static definition of privacy under these circumstances.

---

2 Adapted from a story by Willis H. Ware, The Rand Corporation, in his paper "State of the Privacy Act: An Overview of Technological and Social Science Developments", November 1976.

Attempts have been made also to decide who owns the information and from this, declare what is private and should not be used by anyone else. Presumably if the person is considered to be the owner of all personal facts about him then no one else can have that information without his consent.

There are attractive aspects of this "ownership" approach except that information is intangible and its ownership is not controllable like the ownership of a car, a lawnmower or a book. We cannot control the use of information about one person that another person can obtain simply by observing it himself in everyday life, such as who he is, who he works for, how he spends his money and his spare time, what other people think of him, what his boss thinks of him and an almost endless list of such personal items.

The only way in which some measure of enforceable control is possible over personal information is to restrict access to it and limit the use of information to authorized persons only. As soon as we speak of restricting access to information, we are talking about security.

There is a common expression "...you cannot protect privacy unless you have information security - but just because you have good information security does not mean that you will be able to protect personal privacy". Privacy can be protected by adequate security while personal information is contained within a secure data bank. Information, however, is collected for the purpose of being used and it must be disseminated to various users to serve its purpose. It must, therefore, leave the secure environment where controls cannot be enforced. This might be illustrated in Figure 1.

Protecting privacy while data is held within the EDP environment could be called the technical aspects of privacy protection. The social aspects of privacy protection apply after the data is distributed to users.

Security in an EDP environment involves all aspects of physical security plus several more. This might best be explained by a "ring" concept illustrated in Figure 2.

Administrative and Organizational Security

This includes:

- the organization of security personnel and their appointment to administer the regulations,
- the development and dissemination of security regulations,

- the development of clearly defined reporting channels to proper authority levels and a security awareness and responsibility at all levels,
- determining the sensitivity of the information, the threat to that information, and the appropriate security measures required to counter those threats.

Personnel Security

This includes:

- implementing a thorough personnel security program including a security awareness program for personnel at all levels,
- personnel security clearance procedures (where applicable),
- formal identification of personnel,
- authorization for access to sensitive, classified or personal data only by persons with a need-to-know,
- oaths of allegiance and secrecy,
- personal protection where applicable.

Physical and Environmental Security

This includes perimeter barriers, access controls, locking devices, alarm systems, guard staff, power supply, air conditioning, back-up storage, environmental threats such as water damage, flood, fire and vandalism. The security measures implemented must be consistent with the assets to be protected, the threat posed to those assets and their vulnerabilities.

Communications Security

This is a concern when data is transmitted over telecommunication lines into and out of a data base whether it is a manual or an automated system.

These first four "layers" of security are basic to a secure environment for all types of facilities and must be effective before it is practical to implement the technical aspects of security required by automated systems.

Hardware, Software, Operations and Data

These are the added aspects of security that are required where EDP systems are involved. Hardware, of course, is the equipment, software the instructions, operations are the procedures, and data is whatever it is that holds the data. Firmware is a new descriptive term for what is neither hardware nor software such as a sensor card that can be changed but not with something like a pencil.

DATA SECURITY AND PRIVACY PROTECTION

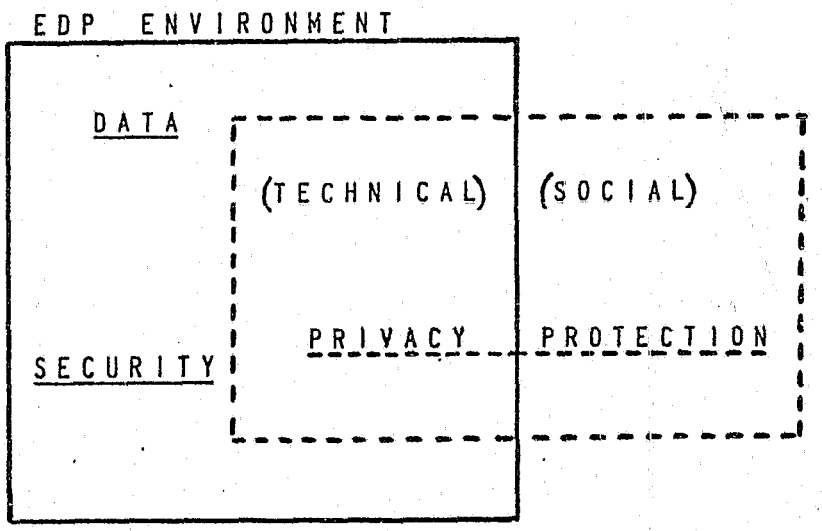

Figure 1

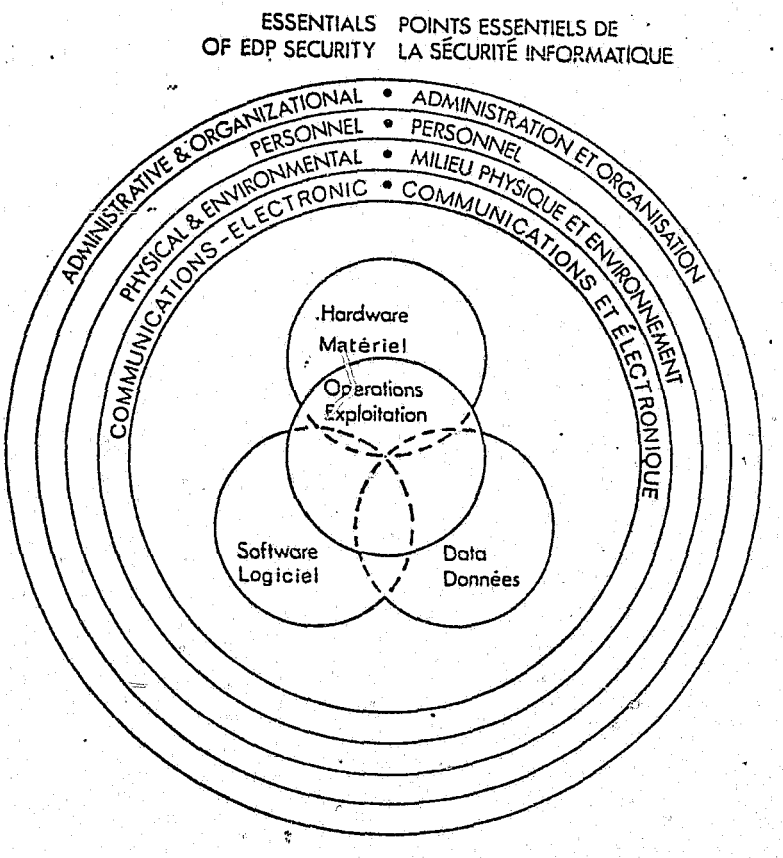

Figure 2

What a system can do or what people can make it do or avoid doing must be controlled and audited to ensure that the data is being used properly and legitimately and by authorized terminals.

When remote terminals have input and output capacity, and particularly where they can alter or purge data, the EDP environment and the security controls must extend to include those terminals and the personnel at remote locations.

All of this takes place within the EDP environment. When it is done appropriately and effectively the information in the system should be protected and be accessible only by authorized personnel. Personal privacy, as it pertains to the personal data within the system, should then be protected. This is the technical aspect of security. It is largely recognizable and controllable.

These physical and technical security controls, however, do not necessarily protect the information, nor the privacy of individuals to whom it relates, after the information leaves the secure EDP environment. When data is distributed to user departments it is out of the EDP environment and into what can be called the social aspects of privacy protection. In this area our approach and understanding of privacy protection is not very precise.

There are probably two aspects of protecting personal privacy at that stage. One is the legislative approach, the other is the ethical or a privacy-principles approach. Neither provide all the answers to protecting personal privacy just as security alone does not ensure the protection of privacy.

Bill C-25, the Canadian Human Rights Act, has passed second reading and is now being studied by the Justice and Legal Affairs Committee. This Bill deals with discrimination and establishing a federal Human Rights Commission. PART IV establishes access rights, for individuals, to personal information about them in federal information systems. See Figure 3. There are certain exemptions from access which are based upon a judgement as to the detrimental affect of such access.

The name of every federal information bank will have to be published in a central index so the public is aware of what exists.

The approach here is to make it possible for individuals to know what information there is about them in federal government departments and how it is being used. In this way, presumably, individuals will have some control over this information and the

C-25

Second Session, Thirtieth Parliament,
25 Elizabeth II, 1976

THE HOUSE OF COMMONS OF CANADA

BILL C-25

An Act to extend the present laws in Canada that proscribe discrimination and that protect the privacy of individuals

Access to and Use of Records

Entitlement of individuals

52. (1) Every individual is entitled to

(*a*) ascertain what records concerning that individual are contained in federal information banks named or otherwise identified in the publication referred to in subsection 51(1);

(*b*) ascertain the uses to which such records have been put since the coming into force of this Part;

(*c*) examine each such record or a copy thereof whether or not that individual provided all or any of the information contained in the record;

(*d*) request correction of the contents of any such record where that individual believes there is an error or omission therein; and

(*e*) require a notation on any such record of a requested correction therein where the contents of such record are not amended to reflect the requested correction.

Where individual to be consulted

(2) Every individual is entitled to be consulted and must consent before personal information concerning that individual that was provided by that individual to a government institution for a particular purpose is used or made available for use for any non-derivative use for an administrative purpose unless the use of that information for that non-derivative use is authorized by or pursuant to law.

C-25

Second Session, Thirtieth Parliament,
25 Elizabeth II, 1976

THE HOUSE OF COMMONS OF CANADA

BILL C-25

Exemption from access

54. The appropriate Minister in relation to a government institution that has control of a federal information bank may provide that subsection 52(1) or any provision thereof specified by him does not apply in respect of a record or part thereof concerning an individual in the information bank where, in the opinion of the Minister, knowledge of the existence of the record or of information contained therein

(*a*) might be injurious to international relations, national defence or security or federal-provincial relations;

(*b*) would disclose a confidence of the Queen's Privy Council for Canada;

(*c*) would be likely to disclose information obtained or prepared by any government institution or part of a government institution that is an investigative body

(i) in relation to national security,

(ii) in the course of investigations pertaining to the detection or suppression of crime generally, or

(iii) in the course of investigations pertaining to the administration or enforcement of any Act of Parliament;

(*d*) would be detrimental to the proper custody, control or supervision of persons under sentence for an offence against any Act of Parliament;

(*e*) might reveal personal information concerning another individual;

(*f*) might impede the functioning of a court of law, or a quasi-judicial board, commission or other tribunal or any inquiry established under the *Inquiries Act*; or

(*g*) might disclose legal opinions or advice provided to a government institution or privileged communications between lawyer and client in a matter of government business.

Figure 3

protection of their own personal privacy. No attempt is made in the legislation to define privacy and no specific conduct or use of information is prohibited on the grounds of privacy violation.

There are two federal Acts in the USA that are already in effect that are intended to make information accessible to individuals. The Privacy Act deals with personal information in federal information systems and the Freedom of Information Act deals with all other types of information in federal information systems. A third Bill, the Koch-Goldwater Bill, HR 1984, will probably be studied by Congress in 1977. This deals with access to information in private-sector agencies. Comparison of the legislation in the USA and Canada would be as set out in Figure 4.

In the USA the involing of an exemption can be challenged in a district court. In Canada a refusal by a department to release information to a person could be taken to the Human Rights Commission which could then investigate the matter. Invoking the exemption by a federal government department may have to be endorsed by the Minister of that Department. If the Minister denies access, that would end the matter; however, the Human Rights Commission will have to submit a report annually on its activities to the House of Commons. The Minister's decisions to invoke an exemption from access could presumably come under question in the House.

The effectiveness of the whole approach of access by individuals, the exemptions possible by institutions and the challenging of those exemptions, as a way of protecting personal privacy, is yet to be demonstrated in Canada.

The collection and use of personal information is increasing. The aggregation of personal information makes it more likely that the records of individuals and their activities will become more detailed. Automated information storage has begun to affect everyone; not just systems like credit reporting agency information, automated police information systems or tax returns. Computers are everywhere, processing such things as motor vehicle registration numbers, purchases, credit accounts, payroll data, personnel records and airline ticket purchases. All of us are recorded in some way in several automated information processing systems and just around the corner there is the electronic funds transfer system, or the cashless society.

All of this aims at the same thing; data capture, processing and use of information by one or more departments. We must surely have to question whether or not legislation will give individuals any real control over this tidal wave of information processing. We are moving headlong into an "information era" with no clear-cut

PRIVACY LEGISLATION

CANADA - U.S.A.

	Access to Personal information within Federal Government Records	Access to Information within Federal Government Records	Access to Information-Public Private, Industrial, Commercial.
UNITED STATES	PRIVACY ACT	FREEDOM OF INFORMATION ACT	H.R. 1984 Koch-Goldwater Bill - Congress to study in '77.
CANADA	CANADIAN HUMAN RIGHTS ACT Part IV	-ACCESS TO FED. DOCUMENTS ACT (PCO study) -Private member's FOI BILL.	---

Figure 4

PRIVACY PRINCIPLES

1. Security within information systems should permit access to data by authorized persons, for authorized uses only.
2. Security should provide protection at a level that is in direct relation to the sensitivity, or the consequences of loss, or misuse of the data.
3. Data should be accurate, complete and current.
4. There should be a commitment to efficiency, (the less information there is, the less there is to protect.)
5. The identity of individuals should be separated from the data, wherever possible.
6. The data subject should have access to information about himself to see, copy and correct unless there is an overriding need within society to prevent this by way of exemptions.
7. Value judgements should not be based solely on information extracted from an information system.
8. There should be an outside monitoring capacity.

Figure 5

answers to how we can protect personal privacy in the process. We have seen that while security is necessary to protect privacy, it does not provide the whole answer. Legislation to provide access by individuals to information about them is also a necessary part of protecting personal privacy but if we look to the future and the uncontrollable expansion of automated information processing systems, we can see that legislation will not likely provide the whole answer either. Something else is needed. As with every aspect of society there must be responsible, accountable conduct and some manner of ethics. How we use information and how we prevent the misuse of information must be addressed. As information becomes more accessible, custodians must become more accountable for how that information is distributed and used. A better defined commitment to protecting personal privacy is probably developing as a result of society's present concern for personal privacy. If there is such a thing as honesty, fair trade practices and business ethics we should be able to develop a set of privacy principles in the processing and use of personal information.

An element of morale suasion must develop to augment the security aspects and the legislative approach to privacy protection. We are just arriving at this approach of ethics or privacy principles as a set of obligations in protecting personal privacy. The Younger Committee on Privacy in the United Kingdom proposed certain principles for handling personal information[3]. Principles such as these parallel some of the elements embodied in existing legislation. A framework for this ethical or privacy-principle approach might be as set out in Figure 5.

As our understanding of personal privacy evolves, the ways in which it might be protected requires continuing analysis. Neither security, nor privacy legislation, nor ethical conduct in themselves will ensure that personal privacy in the processing of personal information will be protected. For the present, the combination of the three is all we have.

---

3 "Computers and Privacy in the Post Office" (Britain), Data Processing Service.

DISCUSSION

S. W. WITIUK: Does the act differentiate between confidentiality and privacy?

R. J. FRIESEN: Neither the Canadian nor the American act attempts to define privacy or confidentiality. The approach has been to consider accessibility by individuals, so this distinction has not been made. I would like somebody to give a definition for privacy or confidentiality that would hold up in all cases.

S. W. WITIUK: I think this may be a definition. Confidentiality concerns the right of access to information already collected. Privacy means the right of individuals to refuse to supply data. In other words none of you might view it as a violation of privacy if someone asked your age. But I might consider that to be a violation of privacy, so it's partly subjective.

R. J. FRIESEN: I agree. One is subjective and another is objective. A woman doesn't usually want to reveal her age. That is a violation of her privacy. Later on, when she wants to collect her old age pension, she will be quite happy to tell her age. Then it's not private any more. So one may definitely be subjective.

T. A. PORTER: I notice the progression from the federal government to the private sector in the United States. Why not involve all government levels?

R. J. FRIESEN: The approach in both Canada and the United States has been towards federal information banks. The approach in the United States now seems to be to look to the private sector, and to require them to reveal information, but there is no mention of any other level of government. In Canada we are moving towards federal-provincial cooperation and are considering information that is in federal systems but which originated in provincial systems. The federal Act will affect the information when it's in the federal systems, but not before, and provindial departments will certainly be interested in knowing how the information will be affected when they give it to a federal department.

D. R. F. TAYLOR: Isn't it also a question of cost? Experience from other countries, in particular Sweden, has shown that when a new service of supplying information to individuals on request was provided the cost was enormous. I think in the Swedish case it increased by 40 percent to 50 percent. I wonder if in Canada anybody had given any thought to the impact of this on existing federal agencies and what it is going to cost the Canadian taxpayer.

R.J. FRIESEN: It's just now being addressed, and not too soon. It should have been done long ago because it is a new application that the system was not designed for. Certainly there's going to be a cost factor, and added personnel. It can be coped with. The technicians will look after that. Each department will have to see how it affects them, since they will be faced with requests for information. Not all departments will have this problem. Certainly some police departments, CPIC, and the RCMP will be concerned. Treasury Board has already assigned a group to examine the impact of this legislation on federal government departments. They are trying to establish common concerns and costs.

D.R.F. TAYLOR: I hope it goes down to the people who will actually build the data banks, because the implications of that type of structure will be enormous.

R.J. FRIESEN: Absolutely.

T.A. PORTER: I wonder if there is an exemption for data such as Statistics Canada holds, since it has data on individuals that are used not for administrative purposes, but for statistical purposes.

R.J. FRIESEN: If it does not identify the individual, I would suppose there is no restriction.

T.A. PORTER: What if it does identify the individual?

R.J. FRIESEN: Then, according to a section of the act, you would have to contact the individual and say you intended using the information for another purpose and he would have to consent to its use. The section would be quite restrictive for secondary uses.

D. SWAN: What procedures would an individual follow in dealing with departments or in legal actions against government agencies?

R.J. FRIESEN: You are getting to the implementation of the act. That will be covered by regulations which have not yet been enacted. Presumably the regulations will establish procedures for persons dealing with a department. I assume that the contact would be directly between the individual and the department.

END