UNIVERSITY OF GUELPH

COLLEGE OF SOCIAL SCIENCES

WORLD CONFERENCE ON ETHICAL CHOICE IN THE AGE OF PERVASIVE TECHNOLOGY

27 OCTOBER 1989

COMPUTERS AND PRIVACY - ESTABLISHED PRINCIPLES: NEW PROBLEMS

UNIVERSITY OF GUELPH

COLLEGE OF SOCIAL SCIENCE

WORLD CONFERENCE ON ETHICAL CHOICE IN THE AGE OF PERVASIVE TECHNOLOGY

27 OCTOBER 1989

COMPUTERS AND PRIVACY - ESTABLISHED PRINCIPLES: NEW PROBLEMS

The Hon Justice Michael Kirby CMG*

DEFINING THE PRIVACY INTEREST

In Australia, we cannot even agree on how to pronounce "privacy", let alone how to define it. The concept is elusive. None of the definitions offered is entirely satisfactory. Most individuals and agencies charged with the task of dealing with privacy related to information technology, try to avoid hard and fast definitions.

Attitudes to privacy vary from one culture to another. Paul Sieghart contrasted, by reference to the work of the anthropologist Hall, attitudes to privacy in several contemporary cultures:

> Germans, [Hall] found marked off their private Lebensraum by closed doors, fences and strict rules about trespass; German law, for instance, forbids the photographing of strangers in public places without their consent. Americans have open doors and no fences, but mark their social

> status with "private" offices and "private" secretaries. The French pack closely together in public, but rarely invite insiders to their homes, even if they know them well. And the English, it seems, rely mainly on their reserve: when an Englishman stops talking, that is a signal he wishes to be left alone.[1]

I am not sure where this leaves Canada and Australia! Sieghart also noted that even within a single society, like the United Kingdom, there are great differences in the extent to which people wish to be able to control the flow of information about themselves. Most people in Britain still wish to keep secret the amount they earn. Inland Revenue officials are sworn to secrecy about the financial affairs of the citizens whom they tax. By way of contrast, all tax assessments in Norway and Sweden are published. Anyone can find out what anyone else earns.[2]

For reasons of history, politics and constitutional law, issues such as abortion, homosexuality and obscenity have been dealt with in the United States under the rubric of privacy. Those who have followed the recent constitutional debates in that country concerning abortion law, will have noted the ways in which the debate is frequently expressed in privacy terms.[3] In other cultures, including my own, such issues are dealt with as sui generis, not matters of "privacy" at all.

Why should we be concerned about the privacy right? Is it simply an attribute of middle-class societies? Or is it an aspect of basic human rights, common to all societies? International statements of human rights, made since the

Second World War, have frequently included references, direct or indirect, to the right to privacy. Thus article 17 of the International Covenant on Civil and Political Rights provides:

> "17.1 No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2 Everyone has the right to the protection of the law against such interference or attacks."

Giving content to the adjectives "arbitrary" and "unlawful" provide much room for debate about the exact scope of the privacy interest.

Some observers contend that when privacy is lost, the subjects become vulnerable to the powers of others. They lose their capacity for self-definition and self-identification. They lose their ability to evaluate themselves, others and situations. They are deprived of attributes of personal autonomy and capacity for emotional release and intimate communication. It is in this way that privacy is justified as a basic human need.[4] Other commentators answer that these assertions are based on scant empirical evidence. In support, they point to the differences in concepts of privacy from one society to another and over time in the same society. For instance, much that forty years ago was regarded as a matter of privacy - social background, possessions, marital status,

nature of illnesses, various sexual matters, facts about relatives and forebears - is sometimes now regarded as non-private, inconsequential, unimportant, even boring.[5]

It was the advent of computers - and the new information technology - that gave a stimulus of urgency to the privacy debate. How this happened was described in the report of the Ontario Commission on Freedom of Information and Individual Privacy in 1980:

> "[T]he broad range of government activity impinges on so many aspects of personal life that the extent of the total personal information holdings of the government vastly exceeds the amount that could conceivably be collected by any single private organisation. Further, there is some public anxiety about the prospect of government ministries and agencies engaging in data sharing or data linkage - drawing personal information from a variety of government data banks and building comprehensive personal files or dossiers on individual citizens ... Finally, the economic and public relations implications of intrusive data surveillance may provide more effective disincentives to its use by business organisations than to its use by government."[6]

Thus it was the advent of big government and big computers that rekindled the debate on privacy. It led to demands in many countries for laws to protect the individual against the risks of loss of privacy as a result especially of the new technology. It also led international agencies to a quest to state basic rules so that these, in turn, might stimulate local law-making and help to harmonize those which were already enacted.

One of the early efforts at defining and exploring the

extent of the privacy interest in the context of computers was that initiated by the Department of Communications and the Department of Justice in Canada. The trail-blazing report Privacy and Computers[7] in 1972 valuably traced the way in which the very concept of privacy developed from primitive to technological societies. It began with an interest in controlling entry into personal space (territorial privacy). Later it extended to protection from interference with one's person (privacy of the person). Then, it developed to an interest of the person in controlling the information held by others about him or her (information privacy). Finally, with new communications and surveillance technology, there was a need for protection from the added risks of intrusion which technology enhancement presented. In the Supreme Court of Canada recently, in the Dyment case to which I will return, privacy interests have been catalogued as "spatial, personal and informational".

It was the concept of privacy in the informational context that engaged the attention of the Canadian committee. Its work influenced a great deal of the work that followed in many lands, including my own. As computers penetrated Canadian, Australian and other societies, people became alert to the issue of "information privacy". The possible need for new law soon became obvious.

PRIVACY THREATENING FEATURES OF COMPUTERS

Computers were not the only sources of the modern threat to privacy. I have already mentioned the increasing

power of government with which came increasing legal powers of intrusion by officialdom. But there were also new business practises such as intensive marketing, private investigators and security officers, the cashless society and the modern credit reference system. The powers of invasive technology to operate surveillance enhanced the penetration of snoops - official and unofficial. The very pace of change in information technology created a problem. Most of the effects of this change were, of course, positive and beneficial. Yet the marriage of computers with telecommunications, producing the era of "computications" brought new dangers for privacy which were soon recognised. The cost per function of a chip dramatically reduced by more than ten thousandfold in fifteen years. Satellite costs per circuit year dropped from $30,000 in 1965 to $700 in 1980. Now they are a fraction of this. The cost of satellite earth terminals fell in like proportion. The cost per byte of memory was fractioned. The capacity of a single optic fibre, one fifth of the thickness of human hair, to do work formerly carried by ten thousand ordinary telephone wires produced such an enhancement of data flow that the burgeoning quantity of information produced risks that information would increasingly be readily available in great quantities about all of us.

These then were the background facts to the penetration of computications in modern societies like Canada and Australia. The universal features of information technology

promoted a heightened concern about the privacy interest. The sources of that concern have been identified many times. The most prominent of them are these:

* Amount: Computers can store vastly increased amounts of personal information and can do so virtually indefinitely, so that the protection which formerly derived from the sheer bulk of records disappears. The computer can retain infinitely vast quantities of information about every member of society.
* Speed: Recent technology has increased enormously the speed and ease of retrieval of information, so that material which was once virtually inaccessible, because it would take too long or be too difficult to get to, is now retrievable, virtually instantaneously.
* Cost: The substantial reduction in the cost of handling, storing and retrieving personal information has made it possible to keep vast amounts of personal information indefinitely. Living it down become much more difficult. Updating accessible old records and reviewing their current relevancy, becomes much more important.
* Linkages: The establishing of crossed linkages between different information systems is perfectly feasible. The capacity to "search"

for a particular name or particular person or features and to "match" identified characteristics was generally not possible in large scale manual record systems. It is now readily possible with modern informatics.

* Profiles: It is now perfectly possible to build up composite "profiles" which aggregate the information supplied by different sources. Yet unless the data which is aggregated is uniformly up to date, fair and complete, the composite may be out of date, unfair and distorted. If decisions are made on the basis of such disinformation, they may be erroneous or unfair.

* New Profession: The new information technology is very largely in the hands of a new and varied employment group, not subject to the traditional constraints applicable to the established professions nor yet subject to effective and enforceable regulation by a code of fair and honourable conduct.

* Accessibility: The very technology and the language, codes and occasional encryption used make unaided individual access to the information difficult if not impossible. In some circumstances these features act as a privacy protection. If proper safeguards are built in, information held in the computerised

office can be more secure from unauthorized access than the conventional office. But proper safeguards are not always provided. The establishment of cross-linkages between different information systems increases the vulnerability of information systems to technologically sophisticated attack.

* Centralization: Although technologically, computerization linked with telecommunications may facilitate decentralization of information, it is prone, by linkages, to succumb to ultimate centralisation of control. This development has obvious political as well as legal implications. Technologically, there is little to prevent state authorities gaining access to intimate personal details about everyone in society. Our present defences against this happening are political and cultural. There are few legal inhibitions.

* International: The advent of rapid progress in international telecommunications, including satellites, and the exponential growth of transborder flows of information, including personal information, make it relatively simple to store intimate personal information on the citizens of one country in another country, not readily susceptible to the enforcement of

protective laws of that country yet instantaneously accessible by reason of the new technology.[8]

The threats to privacy deriving from these and other features of computers, together with the increasing number of public expressions of fear and complaints to agencies which would receive them, led ultimately to the national and international initiatives which I have mentioned.

BASIC RIGHTS AND THE OECD GUIDELINES

There is no specific reference to "privacy" in any of the old statements of fundamental human rights and freedoms, such as Magna Carta, the English Bill of Rights, 1688, the French Declaration of the Rights of Man and of the Citizen (1789) or the Bill of Rights in the United States Constitution (1789-91).

At the conclusion of the Second World War, the United Nations Charter made several references to human rights and fundamental freedoms. There was an affirmation of faith "in fundamental human rights, in the dignity and worth of the human person, in equal rights of men and women and of nations large and small". The Universal Declaration of Human Rights adopted in 1948 accepted as a goal the promotion of respect for rights and freedoms. Article 12 provided:

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

The Universal Declaration was the inspiration for privacy articles which began to appear in regional and other statements of human rights. The European Convention on Human Rights of 1950 included in article 8 a guarantee of the "right for respect for ... private and family life". Article 17 of the International Covenant on Civil and Political Rights in 1966 included the right to privacy already mentioned. The Nordic Council and later the Council of Europe adopted principles for the protection of privacy in relation to automated and non-automated information systems. Finally, in September 1980 the Council of the OECD adopted a recommendation of an expert group concerning guidelines to be followed governing privacy protection in the context of transborder data flows.[9] At the time, Australia, Canada, Ireland, Turkey and the United Kingdom abstained. Since that time, however, all of these countries have signified their concurrence in the guidelines.

The OECD guidelines on privacy are now well established as a body of international principle. Their debt to the earlier guidelines produced by the Council of Europe in particular was obvious and was acknowledged. The guidelines were presented as a consensus document "which can be built into existing national legislation or serve as a basis for legislation in those countries which do not yet have it".[10]

The preface to the OECD guidelines noted that the privacy protection laws had been, or would be, introduced into a number of OECD member countries to prevent violations

of fundamental human rights in the context of changes in the technology of information processing. The OECD Council recommended that member countries take the guidelines into account in their domestic legislation; endeavour to avoid creating (in the name of privacy protection) unjustifiable obstacles to transborder flows of data; and co-operate in the implementation of the guidelines and the adoption of specific procedures for consultation and co-operation upon them.

The OECD guidelines were in the following terms:

Collection limitation principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others a are not incompatible with those

purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except:

(a) with the consent of the data subject; or

(b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) To have communicated to him, data relating to him

(i) within a reasonable time

(ii) at a charge, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.[11]

UNIVERSAL IDENTIFIERS, TAX NUMBERS AND SIN

The OECD guidelines have been very influential in a number of jurisdictions, including in Canada and Australia. In Australia, with some modification, they became the basis of the "information privacy principles" established by the Privacy Act 1988 (Cth). That Act established the office of the Privacy Commissioner within the Human Rights and Equal

Opportunity Commission of Australia. The Commissioner is empowered to make privacy protection measures in relation to Federal governmental departments and agencies. He has specific responsibility in relation to the national tax file number. His functions include encouraging corporations to adopt privacy guidelines. The information privacy principles apply, by force of the Privacy Act, to Federal departments and agencies. A breach of the principles is treated as an "interference with privacy". An individual alleging such an interference may complain to the Privacy Commissioner.

The present Federal government in Australia came into office with an undertaking to accept the OECD guidelines. In due course it did so in the Council of the OECD. There was some delay in the introduction of privacy legislation. Originally, legislation likewise based upon the OECD guidelines and applicable to Federal departments and agencies, was introduced in the context of a proposal to establish a national personal identifier for Australia with the catchy name "the Australia card". As shown by opinion polls, this proposal at first had the support of substantial majorities in the Australian community. A Federal election was fought when the Senate refused to pass legislation to provide for the Australia card. The Senate was content to pass the Privacy Act. But the government insisted that it was cognate with the Australia card legislation. In the event, the Government won the election. But it still did not have a majority in the Senate. A flaw had appeared in the

legislation which opponents gleefully called to notice. Meanwhile, public opinion had shifted. Large demonstrations in all parts of the country signified deep concern about the "Australia card". Ultimately, the Government quietly abandoned the proposal.

Later the Australian government introduced the tax file numbers by an amendment of the Income Tax Assessment Act in late 1988. Under the provisions of this Act, a person involved in certain transactions has the "option" of providing his or her tax file number for inclusion in information reports made to the Australian Taxation Office. The provision of the number is not compulsory. But a decision not to quote the person's tax file number results in an amount being withheld from any payment of relevant income to that person at the maximum rate of tax. This applies to salary and wage income, dividends, interest and unit trust distribution entitlements.

The tax file number system has been justified as a means of eliminating welfare fraud and tax avoidance in Australia. Its object is to provide linkages of information about individuals from various sources. The effective "obligation" to quote the tax file number on most financial transactions will assist the taxation office readily to detect nondisclosure of sources of income. It is a good example of the way in which new computer technology can be used to facilitate the matching of personal records. The Australian Privacy Act was introduced to coincide with

the tax file number system. Politically, it was provided to still the fears of those who saw the new system as an unwarranted invasion into personal privacy.

In Canada, recent debates relevant to computer privacy have concerned the social insurance number (SIN). The last report of the Privacy Commissioner for Canada (Mr John Grace) records, with approbation, the Canadian government's commitment to restricting its own uses of SIN. Some present uses are to be discontinued over five years.[12] Commercial fishermen seeking permits, taxpayers applying for fuel tax rebates, candidates for grants and fellowships are to be "set free" from the "usages of the SIN". With grim humour, the Privacy Commissioner comments:

> "It is something of a paradox that an age which has all but lost the concept of sin has so come under the sway of SIN. Babies have been given SIN as a birth registration number in Prince Edward Island and some funeral directors are said to ask for the SIN of the deceased: thus SIN from cradle to grave; SIN even unto death".[13]

The Commissioner, however, comments, that there have been steps backwards in Canada in relation to the SIN. Under amendments to the Income Tax Act, Canadians are now required to disclose their SINs to financial institutions where there had been no such compulsion before. The new policy, as with the tax file number system in Australia, was designed to facilitate the reporting of interest income to Revenue Canada. Unfortunately, comments the Commissioner, little or not effort was made to notify the public in advance of the

purpose of the collection and use of the number. No effective consultation took place with the Privacy Commissioner before the legislation was introduced. No special consideration was given in Canada to the inherent privacy dangers of SIN. The Privacy Commissioner is very critical:

> "Another precedent is established here. Until these income tax amendments, Canadians were required by law to give their SINs only to the Federal Government. Now they must confess their SINs to banks, trust companies, stockbrokers, credit unions whenever and wherever they make what looks like an interest bearing investment. Welcome to the computer society."[14]

PRIVACY, AIDS AND HUMAN IMMUNO DEFICIENCY VIRUS

Another remarkable indication of the similarity of concerns on both sides of the Pacific is found in the new attention to the problem of AIDS. In countries without a national health system providing universal health cover (such as the United States) great injustices will be done and much hardship suffered by people with HIV and AIDS who slip out of the "net" provided for the old or very poor. Many of the HIV/AIDS patients do not fall within these categories. But in countries with such health systems, such as Australia and Canada, the risk of centralisation of highly sensitive data brings its own rather different problems. Each blood test for HIV may have an indicator for medical benefits purposes. Tracing all those who have undergone a blood test for that purpose, or those who repeatedly do so or are otherwise

involved in HIV/AIDS related treatment, will be a relatively simple function for the benefits paying computer.

In Canada, the Privacy Commissioner has developed recommendations to ensure that HIV/AIDS related personal information is handled by Federal government agencies in accordance with the letter and the spirit of the Privacy Act. A special report AIDS and the Privacy Act has been produced. As that report and other reports on the subject point out, the provision of guarantees of privacy (and against discrimination) to patients with HIV/AIDS is not only a matter of human rights and respect for their individual integrity. It is also the only effective means available to our communities at the present to ensure the full co-operation of the groups most at risk of HIV/AIDS. Those groups are frequently already stigmatized by laws or social attitudes. Their isolation presents particular risks of isolation from the necessary information and reinforcement to help them to help society contain this epidemic. The Canadian report urges particular attention to the development of comprehensive policies on HIV/AIDS in the workplace in the employing agencies of the government of Canada. It calls attention to the strict limitations in the Privacy Act, upon the disclosure of personal information to third parties without the consent of the subject.[15]

In Australia, the Privacy Commissioner has already taken an important role in public discussion about the need for privacy protection in the context of AIDS and government

computers. His relevance to modern Australian consensus is demonstrated by the recent shocking news of widespread leakages of personal data from Federal government records to private investigators. The Privacy Committee of New South Wales, the longest established statutory body in Australia dealing with privacy has prepared guidelines for testing for antibodies to the HIV virus. The latest annual report of the Privacy Committee contains detailed discussion of this issue: another indication of the commonality of the privacy concerns of Canada and Australia.[16] As long ago as 1928 the Canadian Supreme Court affirmed the high value which Canadian Society places on the confidentiality of health information. Justice Duff, speaking for the majority in Halls v Mitchell said:

> "It is perhaps not easy to exaggerate the value attached by the community as a whole to the existence of a completely trained and honourable medical profession; and it is just as important that patients, in consulting a physician, should feel that they may disclose the facts touching their bodily health, without fear that their confidence maybe abused to their disadvantage."[17]

TWO CASES: GOOD AND BAD NEWS

Because of the alarm and fear that attends the development of AIDS, the need for particular security in the processing of data relevant to an individual's HIV/AIDS status is plain. Yet during the past year the courts in Canada have made it clear that the individual has no property, as such, in information. In Stewart v The Queen, the Supreme Court of

Canada overturned a majority opinion of the Ontario Court of Appeal in that case. A union was attempting to form a group at a hotel. It was unable to obtain the names and addresses of the six hundred employees. Management refused to supply this information on the grounds that it was confidential. A consultant, hired by the union, obtained the list through a security guard. For a fee, that guard copied the names from a list in the hotel, without removing or in any way altering the original document. The consultant was charged under the Canadian Criminal Code with counselling to commit fraud, theft and mischief to the private property of the hotel and its employees. The Supreme Court of Canada held that there was no offence. Justice Antonio Lamer wrote the Court's opinion:

> "Confidential information is not of a nature such that it can be taken because if one appropriates confidential information, without taking a physical object, for example, by memorising or copying information ... the alleged owner is not deprived of the uses or possession thereof" ... One cannot be deprived of confidentiality because one cannot own confidentiality."[18]

This decision has been criticised by Mr Grace as having "alarming implications for the information society in general and the Privacy Act (of Canada) in particular". The Privacy Commissioner comments that the "fine legal point of whether one can own confidentiality is simply irrelevant to the important business of keeping sensitive information confidential".[19]

During the same year, the Supreme Court of Canada in the Queen v Dyment[20] asserted that "privacy is essential for the well being of the individual". It stated that "restraints imposed on government to pry into the lives of citizens go to the essence of a democratic state". Referring to the guarantee of privacy in Canada under section 8 of the Charter of Rights and Freedoms, Justice La Forest said:

> "If the privacy of the individual is to be protected, we cannot wait to vindicate it only after it has been violated ... Invasions of privacy must be prevented and, where privacy is outweighed by other societal claims, there must be clear rules setting forth the condition in which it can be violated."[20]

This ringing affirmation of the importance of the privacy right draws strength from the Canadian Charter of Rights and Freedoms. Countries like my own which do not have such a charter must depend upon the common law to guard the privacy right. In the age of intrusive governments, prying business and the great computer enhancement of privacy invasion, the common law - and even the Charter - may sometimes be inadequate champions.

THE INSTITUTIONAL PROBLEM - CAN DEMOCRACY COPE?

It is clear that privacy will take on a new meaning in the age of informatics. Even the OECD privacy guidelines need revision ten years after their adoption. They were framed in terms of the technology of the time by which information was generally supplied for a purpose. Now matters of data can be analysed and identifiers which were

never intended can be established simply by the operation of the new searching capacity of modern information systems.

The lesson is plain. The technology of computications presents very great challenges to the privacy value of societies like ours. The events of recent times pose for us a most important institutional question. It is whether the democratic processes of lawmaking (particularly in Parliament) can keep pace with the dramatic changes of technology which informatics present to nations and to the world. If we are not to be lurched headlong by the chariot of technology but are to preserve our basic values - and protect them by law - we must do better than we have in the recent past. The hare of technology rushes ahead. The tortoise of legal protection dawdles aimless, lost, bewildered, far behind.

FOOTNOTES

* President of the Court of Appeal of New South Wales, Australia. Governor of the International Council for Computer Communications. Commissioner, International Commission of Jurists. Commissioner, WHO Global Commission on AIDS.

1. P Sieghart, Privacy and Computers, 1976 cited Australian Law Reform Commission, Report number 22, Privacy, AGPS, Canberra, 1984, 11 (ALRC 22).
2. Sieghart, 18.

3. Roe v Wade, 410 US 113 (1973) reversed in part in William L Webster v Reproductive Health Services et al, 106 L Ed 2d 410 (1989) (US Supreme Court).
4. J Blousten, "Privacy as an Aspect of Human Dignity" 39 NYUL Rev 962 (1964).
5. H J McCloskey, "Privacy and the Right to Privacy", 55 Philosophy Quarterly 17 (1980) 34, 38.
6. Ontario Commission on Freedom of Information and Individual Privacy, Toronto, 1980.
7. Canada, Department of Communications and Department of Justice, Ottawa, 1972.
8. ALRC 22, 52-3.
9. Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris, 1981.
10. Ibid, 5.
11. Stated in ALRC 22, 270-2.
12. Canada, Privacy Commissioner, Annual Report 1988-9, 6.
13. Loc cit.
14. Ibid, 7.
15. Ibid, 14.
16. New South Wales, Privacy Committee, Annual Report, 1988, 20. See also discussion in Royal Society of Canada, AIDS: A Perspective for Canadians, Background Papers, 1988, 374 ff.

17. [1928] SCR 125. See discussion M Mackinnon and Ors, "Legal and Social Aspects of AIDS in Canada" in Royal Society of Canada, op cit, 374.

18. (1988) 41 CCC (3d) 481 (Supreme Court of Canada) cited in Privacy Commissioner's Annual Report, 2. See also R v Gold [1988] 2 WLR 984 (HL).

19. Ibid, 494.

20. (1988) 55 DLR (4th) 503; [1988] 2 RCS 417 cited in Privacy Commissioner's Annual Report, 2.

21. Ibid, 522.