COMPUTERS AND THE LAW

THE CENTRE FOR CONTINUING EDUCATION, MONASH UNIVERSITY

24-25 MAY 1977

DATA BASES AND PRIVACY

OR HOW TO STOP TALKING AND DO SOMETHING

Hon Justice M D Kirby

May 1977

COMPUTERS AND THE LAW

THE CENTRE FOR CONTINUING EDUCATION, MONASH UNIVERSITY

24-25 May, 1977

DATA BASES AND PRIVACY
OR HOW TO STOP TALKING AND DO SOMETHING

The Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission

PRIVACY IN THE COMPUTER AGE

Some More About the Nature of Privacy

When the Report by the Canadian Task Force on *Privacy and Computers* said that privacy was "undoubtedly one of the more confusing concepts of our contemporary culture" it was an understatement.[1] Put generally, privacy is a value which most western liberal societies would claim. The great liberal philosophers have had little if anything to say about it. Locke, Kant and even Mill never specifically addressed themselves to defining privacy or exploring the contents of the notion. Most of what has been written on the subject has been written by lawyers, especially lawyers in the United States.

The Judeo-Christian tradition lays great emphasis upon the notion of an inner sanctuary and a private sphere of human relationship with the deity. The family unit and the extended family of friends and confidants represent a circle within which

man is able to express sensitive feelings and innermost thoughts without fear of reprisal. But even within a family, members can claim privacy from one another. Definitions in terms of the family unit are inadequate.

In legal writing, privacy is variously described as a right, need, claim, condition, fact, interest, value or ability. This very variety of language underlines the diverse components of the notion of privacy and the lack of precision with which the word is used. It can be used descriptively of facts or as a principle invoking a particular standard of civil rights. To say that a person is in the "privacy" of his home describes a fact. It is when privacy is claimed as a "right" or an "interest" that demands are made for the law to protect it.

This is not the occasion to analyse the features of this so-called "right". It has been done and will be done by the Law Reform Commission elsewhere. In fact, the point of this paper is that there has been too much talk of a general kind about privacy and about protecting it. The time has come for action, including legislative action. It is necessary, however, to sketch very broadly the main features of privacy which should be in the minds of those who are designing legislation to protect this value in the computing age.

Privacy is not an overriding, universal principle. It is not an absolute. A society in which there was total lack of privacy would be intolerable. A society in which there was total privacy would be no society at all. It can be seen as no more than a conditional "right", to be balanced against other needs

and demands which will sometimes override it. These will include the need and demand for information. When it comes to legal machinery for evaluating competing claims, a number of points are clear. First, we cannot allow the scope of a person's privacy to depend entirely upon his own judgment, however keenly he feels about the matter. It would be unacceptable to frame legislation to protect privacy to suit the paranoid or schizoid in society. Nor is it appropriate for the law to deal with every trivial intrusion into privacy. Legal machinery should be reserved to remedy substantial misconduct. The limits of the law should also be recognised. It will never be possible for the law to provide redress for every vague feeling of dissatisfaction about the collection of data or for irrational fears about computers and the potential threat which they pose. Social *mores*, including "good manners" and "self discipline" will always play a vital extra-legal role in the front line of protecting privacy.

At the core of the concern for protecting privacy is concern for the individual human being. Put negatively, it will involve preventing non-consensual intrusion into the individual's own circle by others. Put positively, it will involve the control by an individual of the perceptions which others can have about him. In the United States, the label of "privacy" has been attached to most of society's supposed ills. Abortion, motor cycle helmets, homosexuality, hairstyles, marijuana, psychological testing and sodomy have, with greater or less success been brought beneath privacy's convenient banner.[2] We in Australia should resist the temptation to confuse our thinking in this way. Without at this stage attempting an exhaustive definition of privacy, it is enough to

say, for present purposes, that it is one of the values claimed in Australian society and it is bound up with the respect to be accorded to the autonomy of the individual in our society. It is a recognition that there are some things which other members of society do not have a right to know and indeed, in respect of which they have an obligation to let the individual alone. Weighing the competing values, especially the need for information to organise a complicated society is not easy but it must be done. The provision of appropriate machinery takes on a new urgency in the age of computers.

The Computing Dimension : A modern witch?

Much has been written about the "peril" of the computer. One writer has even suggested that the computer has become the modern witch :

> "A retrospective glance at history instructs us that the witch is likely here to stay. She seems to make her appearance when cultures are unsure about the values upon which their institutions are based and frightened about the prospects for the future. Irrational fears, coupled with a predisposition to scapegoat threatening elements to social harmony, bring the witch forward in full display. ... How frustrating it is for children and the child in all of us to find out, when hysteria abates, that the witch is just an ordinary neighbour".[3]

This said, there are undoubtedly implications for privacy in the development of the computer and of the computing resource, which it would be as wrong to ignore as to exaggerate.

It seems generally agreed that just as a person can invade your privacy by entering your home, uninvited and seeing you directly or, standing outside your property and seeing you with sense-enhancing devices or overhearing what you say with such aids, so strangers can "see" you and equally invade your privacy by having available information about you. If privacy is an aspect of the integrity of the individual in our society, it includes the right of the individual, in given cases, to control the perceptions which others have of him, directly and through information.

It is in this respect that a rapid development of computing impinges on privacy. Files of information have been kept since the earliest recorded history of man. However, the computing explosion adds a new dimension. That there is an explosion, can scarcely be disputed. In 1950 there were sixty implements worthy of the name "computer" in the world. It was an intellectual toy. By 1954 there were 5,000. In 1960, 30,000. At present there are probably 100,000. It is predicted by 1980 there will be 200,000 in the United States alone. Eighteen billion dollars will be spent annually on computing. Fourteen percent of the national expenditure on equipment will be devoted to this resource. Two to three million United States citizens will be directly or indirectly involved in the industry. Australia will not be immune from this explosion. But it is

not numbers and equipment alone that works the computing revolution. The rapid drop in average cost of retrieval of information and massive increase in average speed of delivery of information provide the potential for the expansion of computer utilisation for the supply of information.

Although there has been a great deal of loose talk about the so-called perils of computing, a number of features of the computing resource can be identified as posing potential threats to individual privacy.[4] Put shortly, these features are :

* The scale of information storage capacity which becomes possible with computing.
* The rapid speed of retrieval of information.
* The markedly diminished cost of collecting and retrieving information proportionate to this scale and speed.
* The capability of the resource to transfer, combine and multiply information supplied for many different purposes.
* The susceptibility of this resource to centralisation of control, in the name of efficiency and economy.
* The unintelligibility of data in raw form and the need for special training to secure access to and control of it.

Fears and Practicalities

Put bluntly, the fear arising from these features of the computer is that a small group of trained experts will have at their fingertips for instant, inexpensive retrieval a great mass of co-ordinated, consolidated information about each and every individual in society. As against those who have the power to retrieve such information, gathered from the cradle to the grave, the subject will have precious little privacy. Those with control of this information will be able, at whim, to "see" each individual in society through this storehouse of information. The individual's power to preserve control over the perceptions that others have of him will shrink markedly.

Having stated the fear, it is important to avoid the "witch mentality". It is necessary to put the exercise of protecting privacy in the computing age into proper perspective.

Much of the agitation for privacy protection against computers undoubtedly comes from the fear of centralisation of corporate and bureaucratic power. But it will not be possible by legislation dealing with computers, to prevent society falling victim to totalitarian rule. Nor would any such régime respect rules controlling the use of its computers. Our defence against intolerable political and other control must rest elsewhere. Although there is a fairly high level of governmental, corporate and political sensitivity to privacy and the extent to which intrusions will be tolerated, the dangers to privacy probably exist not in a frontal assault by intruders but in the gradual erosion of the area which is respected as the individual's "own business".

It must be remembered that although the fears about the threats to privacy posed by computers were first expressed more than ten years ago, no dramatic increase in privacy invasion has been remarked in the last decade. There has been no dramatic increase in the amount of information of a personal nature extracted from citizens. On the contrary, one of the positive advantages of the debate which has surrounded the computing explosion has been the increased awareness in the community about the collection and storage of information held on its members. The vigorous debate which accompanied the national census in Australia in 1976 bears witness to the public alert that exists in this country. That awareness is in one sense the first line of defence against intolerable intrusions into areas presently marked "private". In another sense, given the increased dimension of potential invasion, it expresses the public demand for adequate legal machinery to provide appropriate protection and redress.

Whilst combatting irrational fears, avoiding witchhunts, escaping individual eccentricities of views about what are and are not private aspects of our lives, two other practical considerations must be borne in mind. The first is that because privacy is neither an absolute nor universal value, perceptions of the interests to be protected by the law will vary in time and place. Take the following table drawn from two surveys conducted on the subject.[5] The first column shows the results of the survey commissioned by the Younger Committee in the United Kingdom. The second is one conducted by the United States Bureau of Standards. Each survey sought to establish what the public thinks is private.

Although direct comparison between the two surveys is not possible, there were certain common features and the table is instructive. It is particularly interesting to see the comparatively high value attached in each community to the privacy of salary level. This evaluation contrasts with the position in Sweden and Japan where tax returns, far from being sacrosanct, are available by law for public scrutiny.

What the public thinks is private

	UK	US
Common features:-		
Salary	78%	42%
Medical	50%	18%
Political activity	40%	47%
Education	19%	19%
Employment	10%	22%
In one survey only:-		
Sex life details	87%	
Address	32%	
Religions	24%	
Tax		20%
Credit Rating		20%
Police		15%

Australia presents a fairly homogeneous society and although there may not be great differences in matters considered private in Perth and Hobart, a moment's reflection teaches the great changes that have occurred even in the past decade concerning what was once considered private and intimate and what is now openly revealed and indeed discussed without embarrassment.

A final practical consideration of great importance is that of cost. A decision must be made in terms of informed

cost accounting as to how much society is prepared to pay in sheer economic cost to preserve and protect its privacy. Schemes of security, rights of access, obligations to supply copies, destruction requirements, the provision of physical security and so on do not come without cost but must ultimately be passed on to the community. Fears about the social and political implications of cross-linkage of data systems produce suggestions for dispersal of information that amounts to a form of planned inefficiency. Obviously, society will be prepared to pay a price for privacy preservation and protection. But in designing the instruments of legal control, it will be important to keep in mind the costs involved, so that these can be weighed continuously against the other values to which society attaches importance, including the spread of information and the economic and efficient use of resources, including the computing resource.

PROTECTING PRIVACY

The Present Position

The man in the Australian street would no doubt assert that he does have a "right of privacy". It would not be difficult for him to identify various parts of his life which he considered to be peculiarly his own business and for which he would claim the right to be free from outside interference or unwanted publicity. We do not have in Australia a collection of our rights equivalent to the United States *Bill of Rights*. According to our conventional legal theory, it is customary for us to assert that freedom of action exists except to the extent that it is impinged upon by the common law or by statute. However, the growing

mass of statute law characteristically *does* include provisions which intrude upon the individual's freedom of conduct and sphere of private activity. Furthermore, the development of bureaucratic practices and methods, serviced now by computing, likewise *does* intrude and the law is perfectly silent, providing neither protection nor redress. Forms to be filled in, files accumulated, information collected, disseminated and stored all erode the seclusion and isolation of the individual.

The common law of England and Australia failed to develop a general right of privacy enforcible in the courts. In *Victoria Racing and Recreation Grounds Co. Limited v. Taylor*[6] Latham C.J. put in this way :

> "However desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists".[7]

The demand for legal protection of privacy in this country arises only in part from public fears about the potential of computing to erode this value. In part, it is the product of a growing demand for more systematic attention to the protection of human rights which received impetus from the abuses revealed in the aftermath of the Second World War. Article 12 of the *Universal Declaration of Human Rights* adopted by the General Assembly of the United Nations in 1948 states that :

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence or with attacks upon his honour and reputation".

Article 17 of the United Nations *Covenant on Civil and Political Rights* is in similar terms. Australia signed the Covenant in December 1972 but has not ratified it. These international percepts are not part of the domestic law of Australia. The international movement and the local recognition that rights of the individual in society may be eroded unless something is done led to the reference in April 1976 to the Australian Law Reform Commission, which is now charged with the responsibility of investigating and reporting upon new protections for privacy in this country, within the Commonwealth's domain. What can be done?

Mechanisms of Regulation

Self-Regulation. There is no doubt that self regulation will play an important part in providing protection to privacy against the feared abuses of computers. Self-regulation can take the form of purely voluntary agreement to regulate aspects of conduct by members of a voluntary organisation. As in the professions of law and medicine, the State may enact legislation supporting the rulemaking and enforcement powers of the professional body. The advantage of self regulation is that it can be amended rapidly, applied flexibly and in detail too minute for satisfactory legal control. In a developing science, such as computing, there are real dangers in attempting with too great precision to discipline detailed aspects of individual conduct.

Nevertheless, both the British Committee considering this problem and the Canadian Task Force[8] concluded that, whilst moves towards self regulation in respect of privacy should be

encouraged, such moves ought not to be relied upon as by themselves, resolving all of the problems and potential problems.

The Courts. The courts, which failed to develop any general theory of privacy are, nevertheless, the traditional guardians of civil rights. But to attempt to meet the privacy and other implications of rapid development of automated information systems by the judicial approach is simply impractical and probably impossible. Litigation is costly and time consuming. Principles are developed slowly and only by those who are able to gain access to the courts. Computer technology is changing rapidly and proof in a curial situation would add to difficulties and expense. Furthermore, it is of the nature of privacy invasions that public ventilation by court processes may be the last thing the victim wants and indeed may be corrosive rather than protective of privacy. The invasions may be minor and nagging. They may even be carried on without the knowledge of the subject. The courts may have a role to deal with serious cases in specified areas and to redress wrongs that have already occurred. More flexible machinery may be needed if day to day regulation and dispute resolution is to be provided in a practical way for the operation of computers and the conduct of the operators.

Administrative Regulation. A number of models already exist for dealing with the privacy aspects of computing operations. Some concentrate on a strategy of behaviour modification. Others establish machinery of dispute and grievance resolution.

Closest to home is the N.S.W. Privacy Committee established

in 1975 following the report by Professor W.L. Morison, prepared for the Standing Committee of Attorneys-General. Professor Morison recommended against the creation of a general tort of privacy for enforcement in the courts and suggested instead legislation to establish a Committee which could research and develop general policy towards privacy. That Committee, set up by Act of the N.S.W. Parliament[9] has a statutory function to receive, investigate and mediate in complaints by any person of unjustifiable invasion of privacy. The Committee has no power to enforce its decisions in a legally binding way. It has no power to grant damages or other like means of redress. Nevertheless it has been able to sort out, by conciliation, a great number of complaints coming to it. It has also been able to establish practical machinery, as for example to permit access to certain credit and criminal records.

There may be much merit in providing, at a federal level, for just such a watchdog committee, commissioner or commission. Recent Bills introduced into the Canadian and New Zealand Parliaments[10] propose that a commissioner of the national Human Rights Commission in each country should have a special responsibility for privacy. The Commonwealth Government in Australia has announced its intention to establish a Human Rights Commission.[11] Perhaps one of the commissioners of this Commission should have a specific role for the protection of privacy. This would have the advantage of ensuring that the federal standards of privacy were developed in a proper context. Because privacy is not an absolute value, it should not be developed in isolation. It should be seen in the context of protection of human rights

generally within our community. The dangers of falling victim to obsessive zeal to protect every imagined encroachment upon privacy are as real as the dangers of standing idly by whilst privacy values are eroded.

The Canadian Task Force Report identifies other alternatives. They include the establishment of an independent administrative tribunal, with a function to licence databanks. This procedure may run into constitutional problems in Australia and may, in any case, amount to a heavy-handed means of dealing with a difficult and complex area. The establishment of a surveillance agency or assignment of surveillance functions to a privacy commission could ensure practical, on the spot superintendence, by appropriate experts, of the respect for privacy in the conduct of computing operations.

Yet another approach would be to deal with specific problems in a specific way. This would envisage specific legislation to deal with the Medibank computer, banking computers, computerised census and statistical information, the computers in the Commonwealth Public Service and other computers under federal jurisdiction. As recognised by the Canadians, the major defect of this approach is the danger that it could lead to a haphazard and uneven protection of privacy under administrative law and the development of ill thought out and unco-ordinated policies all given the name of "privacy".

Criminal Penalties

Because the community as a whole has an interest in maintaining privacy, it may be appropriate to attach criminal penalties for wrongful conduct in the collection, dissemination and storage of information. When corporations were developed, new areas of crime were developed with varying degrees of success and usually by analogy with existing crimes. Crime has not remained aloof from the computer. There have already been major instances of computer theft and computer fraud. Is it appropriate, to protect the community value of privacy, to attach criminal sanctions to at least some ethical rules designed to preserve the security and confidentiality of sensitive, personal information? Are such developments necessary in order to provide the lowly operator at the end of the computing chain with a proper line of defence, to which he can retreat when asked to perform conduct which he regards as wrong because it involves the invasion of the privacy of another?

Principles for Enforcement

Seven Principles. Whatever the actual machinery proposed to regulate or licence databanks, to investigate, conciliate and resolve complaints and disputes and to police the day to day respect for privacy, some broad principles must be determined which the machinery can help to operate. In his 1977 Cantor Lectures, David Firnberg, the Director of the National Computing Centre in England identified seven requirements that emerged from an analysis of international attempts to provide privacy protection in the computing age.[12] It may be helpful to summarise them, so that we can consider their application to our Australian inquiry.

1. Personal data shall be *declared to exist* either by a publicly available register of all systems or by separate notification to individuals that personal data exists about them.
2. Personal data shall be *specified in terms of its content* i.e. containing identifying information that links the record to a particular individual.
3. The *purposes for the use* of information shall be described and if there is a licensing of a databank system (as in Sweden) the *use* shall be predeclared and other uses not permitted.
4. Personal data shall be *accurate, relevant and complete* i.e. shall be the minimum necessary for the stated purpose, up to date and subject to correction without delay, where wrong.
5. Personal data shall be protected by *security*. This will include the assignment of personal obligations to those responsible for holding personal information, the provision of technical and organisational methods of physical safeguards to ensure security and confidentiality of records.

6. Personal data shall be of *limited life*. This implies that a record should be kept of the age of such data and, where not in conflict with other legislation providing a different period of time, such personal data will be erased when its purpose has been fulfilled.

7. Personal data shall be *depersonalised for statistical use*. It has frequently been pointed out that necessary protection of the poor and minorities of all kinds require the removal, under security, of links between individuals and general statistics.

Federalism and Trans-border Flows. As if the problem were not sufficiently complex, we face in Australia the additional special difficulty that it is probably not within the power of the Commonwealth Parliament to enact general legislation governing the use of computerised databanks throughout Australia. I say "probably" bearing in mind the doubts which exist in relation to the scope of the External Affairs power[13] and because effective dominance of this particular aspect of privacy might well be possible under the telecommunications power and the corporations power of the Commonwealth.[14] Plainly, the Commonwealth will have ample power to enact legislation controlling databanks, manual and computerised, in use in the Commonwealth's own public service, by its agencies and instrumentalities. There will also be plenary power to enact legislation in respect of the government and private databanks in the Commonwealth Territories. Beyond this, the

protection of privacy will have to be left to the States. The potential for evading privacy protective controls by trans-border data flows has already attracted the attention of the Council of Europe and the O.E.C.D. Whilst our problem is not as acute as Canada's, a growing amount of private information about Australian residents is collected and stored overseas and may require specific attention.

Hard Decisions

A number of hard decisions stand out for practical consideration and answer by the Law Reform Commission. The answers will have to be practical because they will be addressed to the Parliament which will have the obligation of considering what can and ought to be done by the Commonwealth to protect privacy in a community in which use of computing grows apace and is unlikely to abate.

Can I suggest that the following questions in particular stand out :

1. *Self Regulation.* What role is there for self regulation of the computing industry and by whom should it be done? Is the Australian Computer Society a suitable vehicle? Should there be statutory support for discipline imposed? Should there be "swearing in" of computer personnel? Should ethical training be insisted upon and, if so, how should it be given in such a diverse industry?

2. *General Regulation*. Should there be some form of general regulation to catch the multiple invasions of privacy that can occur? If so, is it apt to commit this to the courts by means of a statutory tort of privacy or should a regulatory agency of some kind be established, after the model of the Privacy Committee of N.S.W., the Ombudsman or the Administrative Appeals Tribunal?

3. *Principles of Legislation*. How far are the seven principles set out above applicable for Australian legislation? Are any of them unacceptable? How can they be implemented in practice? Implementing them, what form should the legislation take, not simply to state principles in general terms but to provide in a detailed way for their adoption in practice?

4. *Sanctions and Remedies*. In part, the sanctions and remedies provided will depend upon the machinery adopted to receive and conciliate complaints, enforce decisions in the case of dispute and punish offences. The range of available options is great. Should it involve civil action by the complainant or by the regulatory agency itself before the courts? Should it involve the suspension of licences, orders for

compensation, injunctions against repetition, declarations of publicity concerning mistakes that are made? If criminal sanctions are to be introduced for privacy invasion what should be their terms and to whom among the computer personnel should they apply? Should criminal offences be reserved for really serious cases of deliberate and wrongful invasions of privacy? What form of policing of privacy standards is appropriate? Is a surveillance or monitoring body of mixed experts appropriate or can this problem be left to police authorities to enforce the law?

5. *Differentiation.* Three problems at least of potential differentiationof treatment arise for consideration:

   * Manual files v. computerised data.
   * Government standards v. private sector standards.
   * Commonwealth standards v. State standards.

   Is it right in principle that invasions of privacy held in manual files should be ignored? Does the computer dimension add a special new discrete problem which calls for new statutory initiatives? Is it appropriate that the machinery for

resolving disputes and maintaining surveillance in respect of Federal Government databanks should be different from rules for the resolution of complaints against other databanks in the private sector? Given the problems of trans-border data flows, is it apt to leave the general control of automatic computerised data to the States or is it desirable for the Commonwealth, by use especially of the telecommunications power, to seek a common uniform standard throughout Australia? Is there protection for privacy in disparate State laws in this area or do the different standards encourage the collection of computerised information in those parts of the Commonwealth having the lowest protections for privacy?

There are, of course, very many other issues but enough has been said to outline some of the problems that face the Law Reform Commission. The international movement for protection of the individual and particularly individual privacy against the information explosion facilitated by computers has reached Australia, somewhat belatedly. The Commission performs its functions in the open and after proper consultation with the Australian community, including the expert community. This national conference provides

an occasion for interdisciplinary contact which is of vital importance for any informed reform of the law. The Attorney-General has already appointed computing personnel as Consultants to the Commission, to assist it in its inquiry. Further such assistance will be secured before we report. I avail myself of this opportunity to direct the legal and computing communities to the hard decisions that will have to be made. I invite the assistance of each profession and of the wider Australian audience in providing the Parliament with the answers to these hard questions.

FOOTNOTES

1. *Privacy and Computers*, a Report of a Task Force established jointly by the Department of Communications and Department of Justice, Canada, 1972.
2. D. Weisstub, *Computers and Privacy*, Paper for the Canadian Bar Association (Ontario) programme on "Computers and the Law : Emerging Issues", 21 Oct. 1976, *mimeo*, pp.6-7, citing C. Lister.
3. *ibid*, pp.21-2.
4. *Computers and Privacy*, Home Office, London, 1975, Cmnd. 6353; *Computers : Safeguards for Privacy*, Home Office, London, 1975, Cmnd. 6354.
5. This Table is found at p.3 of D. Firnberg, *Computers and Privacy*, Cantor Lectures, 1977, Lec.I, 21 March 1977.
6. (1937) 58 *C.L.R.* 479.
7. *ibid*, at p.496.
8. Especially Canadian Task Force, p.168.
9. *Privacy Committee Act, 1975* (N.S.W.)
10. Bill C-25, *Canadian Human Rights Bill, 1976*, Clause 57; *Human Rights Commission Bill, 1976* (New Zealand); clause 58(1)(a).
11. Announcement by the Commonwealth Attorney-General, Mr. Ellicott, on 26 December 1976, *mimeo*, 90/76, p.2.
12. Firnberg, pp.12-14.
13. Re the Judge of the Australian Industrial Court & Another : Ex parte *Ex parte C.L.M. Holdings Pty. Limited & Another* (1977) 13 *A.L.R.* 273.
14. *ibid*, Mason J.