I.C.L. COMPUTER USER CONFERENCE

6TH BI-ANNUAL CONFERENCE 20-23 OCTOBER 1981

WREST POINT, HOBART, 21 OCTOBER 1981

TOWARDS EFFECTIVE FEDERAL PRIVACY LAWS

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

September 1981

I.C.L. COMPUTER USER CONFERENCE

6TH BI-ANNUAL CONFERENCE 20-23 OCTOBER 1981

WREST POINT, HOBART, 21 OCTOBER 1981

TOWARDS EFFECTIVE FEDERAL PRIVACY LAWS

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

THE TECHNOLOGICAL SOCIETY

We live in a remarkable time. History will record that the chief dynamic of our generation was an extraordinary explosion of technological development. Almost every task given by the Federal Attorney-General to the Australian Law Reform Commission reflects a recognition of the impact of science and technology on the law and the need both to use science and technology in the law and to provide safeguards against dangers created by them.

Our project to reform criminal investigation procedures of Federal police required us to examine the ways in which technology could be brought to the aid of the criminal justice system accurately and fairly to resolve disputes and uphold the truth in criminal process. To this end we recommended sound recording of confessions alleged to be made to police. We recommended photography and video taping of identity parades, to assure the jury that they were conducted fairly and to guard against wrong identification. We recommended in favour of telephone warrants, by which judicial officers could authorise urgent arrests and searches by telephone. In our report on Alcohol, Drugs and Driving, we recommended new breathalyser equipment and additional facilities for the police to secure body samples for testing against intoxicants other than alcohol. In our report on Human Tissue Transplants, we had to deal with one of the remarkable biological developments of our time. From the beginning of recorded history, the human body has rejected the transplantation of organs and tissue from another. In our time, medical technology has overcome the immune reaction. Acute moral and legal problems are posed. When is the donor dead? Should we all be deemed to be donors or should consent be required? Should young children ever be permitted to donate non-replaceable organs such as kidneys?

In our report on defamation law reform, we had to address a national problem created by new broadcasting technology. When defamation was a hurt hurled over the back fence, it was apt to have a local State law dealing with the problem. With the development of fast distribution of print media, telefacsimile, radio and television, telex and other means of telecommunications, defamation can be distributed nationally. The technology creates a new legal problem and the need for a new, national answer.

Our project on debt recovery laws requires us to look at a world of bankcards, automated credit reference systems and electronic fund transfers. Our project on the reform of evidence law in Federal Courts requires consideration of modern psychological evidence. Some of the assumptions on which our evidence law has been based are simply not borne out by modern empirical and scientific research. The admission of computer evidence, the product of many hands, offends against the hearsay rule: for who can cross-examine a computer? Yet disharmony between the laws permitting evidence to be given in the courts and the fast developing rules governing business and other information practices will only bring the law and its institutions into contempt. The hearsay rule will not hold back the onrush of the computer. It will be necessary for us in the law to adjust our rules to the wired society.

Of all our tasks none brings us more directly into contact with information technology than our project on the protection of privacy. The problem of privacy in the last decades of the 20th Century and in the 21st Century will not be so much the problem of an intruder looking at you through the keyhole. It will be the problem of data privacy: someone looking at you through your 'data profile', through integrated computerised information stored about you and retrieved for the use of the decision maker.

The society of the new information technology will be highly integrated and therefore, potentially, more vulnerable. There is a need for safeguards against the vulnerability of society as a whole. I refer to:

* criminal acts such as sabotage, espionage and susceptibility to terrorism;
* misuse for political or economic purposes;
* danger from catastrophies and accidents;
* sensitivity of personal and confidential registers;
* functionally sensitive business systems;
* the vital importance of key persons;
* increasing dependence on overseas data processing.

I would also mention two other aspects of vulnerability. The first is the vulnerability of certain groups of employees, who, at least initially, would fall victims to the economies of the new technology. It is about the third vulnerability that I wish now to speak. I refer to the vulnerability of the individual and of individual liberties in the information society. This is the project which is before several law reform commissions in Australia. It is not a local obsession of a few lawyers. It is an international concern of Western communities. It is one of the important problems that must be addressed as new information technology is introduced. The need for safeguards are recognised and are being acted upon in most countries with political and economic systems similar to our own. What should we do?

THE NOTION OF 'INFORMATION PRIVACY'

In a nutshell, the basic problem of information privacy today is that government and business bodies maintain, as a matter of course, a vast amount of personal data on just about everybody in modern Australian society. The collection of such data and its growing computerisation increase daily. Whether it is a social security record, Medibank file, income tax return, credit reference or record of insurance claims experience, we can all be sure that we are 'on file'. In the old days, there was a certain amount of protection for the individual, arising from the fact that files become too bulky and had to be discarded. Linking manual records, kept in differing places, was just too difficult and expensive. Technologically, these problems no longer provide an impediment. Data of almost limitless quantity can be stored. Data from differing sources can be integrated and kept indefinitely.

The legal system long ago developed remedies to protect bodily and territorial privacy. The laws of assault and trespass provide instances of this. If you trespass physically on a person, his land or goods, the law provides enforceable remedies and punishments. Nowadays, we speak of 'information privacy' meaning the individual's 'zone of privacy' relevant to today's world. 'Information privacy' is the claim of the individual to have some control over the way in which he is perceived by others 'on his file'. In a rural society, privacy may be protected, in law, by defending the person, property and territory of individual. In a society of data bases, perceptions of the individual and intrusions upon his personal life will generally have nothing to do with his physical person or immediately surrounding territory. Vital decisions will be made as a result of perceptions of an individual through his 'data profile'. Modern privacy is the business of asserting and upholding the individual's rights in respect of personal data about himself. I repeat, privacy invasion today is a problem of the data base not the keyhole.

THE PACE OF CHANGE

A major difficulty of designing effective machinery for the protection of the privacy of personal information is that the information technology, sought to be tamed, is itself changing so rapidly. One U.S. report recently said that the basic problem was that the 'time cushion' between technological advance and the legal response had simply disappeared. Things are just happening too fast for the slow moving machinery of law making. Alvin Toffler in his recent book The Third Wave says that we are facing a crisis of our law making institutions. They are simply incapable of keeping up with the needs identified by modern technology.

Certainly, things are happening fast. A few recent developments mentioned in the discussion paper are:

* the cost per function of a micro chip has been dramatically reduced by more than 10,000 fold in 15 years;
* satellite costs per circuit year 1965 - $30,000; 1980 - $700;
* satellite earth terminals 1975 - $10,000; 1979 - $12,000; 1980 - $1,000;
* bubble memory 1975 - 256,000 bubbles on a chip; 1979 - 1 million bubbles on a chip; 1980 - 27 million bubbles on chip;
* a single optic fibre one fifth of the thickness of human hair can do the work of 10,000 ordinary telephone wires.

Although these rapid developments are daunting to the layman, and although they necessitate flexibility in any legal machinery that is provided, it has not been the way of our legal system to simply give up in despair. It must be frankly acknowledged that no legal system will provide for the detection, punishment and redress of every privacy invasion which occurs, whether in a data bank, electronic surveillance or otherwise. But the law should provide guidance about fair information practices and flexible and accessible sanctions and remedies to adjudicate such complaints of privacy invasion as are brought to notice. Unless this is done, respect for the individual and his rights to privacy will be continuously eroded. In the process a very important feature of our form of society will be destroyed.

DANGERS OF AUTOMATION

The first inquiries which looked at computerisation of personal data did not consider that any new or special problems arose requiring legal attention. Even today, it is pointed out that damaging personal data can be kept in a notebook or in the bottom drawer. If used at a critical time, it can do great harm to the individual. Conceding the

dangers of old information practices, it is now generally recognised that the new technology results in special features which endanger individual privacy and therefore warrant legal responses, of one kind or another, to protect the individual. What are these features?

* Amount. Computers can store vastly increased amounts of personal information and can do so virtually indefinitely, so that the protection of sheer bulk evaporates.

* Speed. Recent technology has vastly increased the speed and ease of retrieval of information, so that material which was once virtually inaccessible because it would be just too difficult to get at is now, technologically, instantaneously at one's finger tips.

* Cost. The substantial reduction in the cost of handling and retrieving personal information has made it a completely viable proposition to store vast amounts of information of a personal kind indefinitely. 'Living it down' becomes more difficult. Updating accessible old records becomes more important.

* Linkages. The possibility of establishing cross-linkages between different information systems is perfectly feasible. The capacity of computers to 'search' for a particular name, or particular personal features and 'match' identified characteristics was simply not possible in the old manilla folder.

* Profiles. It is now perfectly possible, if access can be gained to numerous personal data bases, to built up a composite 'profile' which aggregates 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 such data, they may be erroneous or unfair.

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

* Accessibility. The very technology, and the language, codes and occasional encryption used makes unaided individual access to the data difficult if not impossible. In a sense the new technology can actually protect security and confidentiality. But privacy depends on who may have access to personal information.

* Centralisation. Although technologically, computerisation linked with telecommunications, may facilitate decentralisation of information, it is prone, by linkages, to ultimate centralisation of control. Obviously, this has implications of a political kind. Technologically, there is little to prevent 'Big Brother' gaining access to intimate personal details of everyone in society. At present, our defence against this happening is political and traditional. There are few legal inhibitions.

* International. The advent of rapid progress in international telecommunications, including satellites, and the exponential growth of trans border flows of data, including personal data, makes it relatively simple to store intimate personal information on the citizens of one country in another country: not readily susceptible to protective laws yet instantaneously accessible by reason of the new technology.

The recognition of these features of the new information technology has led to the development, during the past decade of laws protective of the individual and assertive of his rights in respect of personal information. They began in Germany and Sweden, spread to North American and have now been developed in most European countries. The very universal nature of the new information technology makes it important that we should seek, in Australia, to develop laws which are compatible and consistent with those developed in other countries with which we have numerous telecommunications links. The legal machinery provided in the laws developed to date differ from country to country, in accordance with differing legal traditions. But at the heart of the national and international efforts to reassert the individual's rights in respect of personal data systems, is an idea which is essentially simple. It is an idea which has been adopted by the Australian Law Reform Commission. It is the central provision of the proposals on information privacy protection. It is that normally, with exceptions spelt out by law, the individual should have access to personal information stored which concerns himself. Where this information, on access, is found to be false, out of date, incomplete or otherwise unfair, remedies should be readily available to permit the correction, deletion or annotation of the record. In the future, the individual will be 'seen' through his file. It is vital that legal machinery should be available to ensure that he is 'seen' accurately and fairly. It is also vital that the law should give guidance to those involved in the collection, use and dissemination of personal information. Perhaps I should say that the Tasmanian Government has introduced into the Parliament the Criminal Records (Access) Bill 1981 to confer on persons a right to have access to criminal records kept in relation to them and to provide procedures for review and correction of records found to be incorrect. Clearly this is a step in the right direction.

NEW PROTECTIONS FOR PRIVACY: BASIC RULES

In many of the countries of Western Europe, legislation has been enacted to establish data protection boards, with which every owner or user of computerised systems containing personal data must register or by which they must be licensed. In the United States, Federal legislation enacted as the Privacy Act 1974 is basically enforced by administrative direction and upheld ultimately by private civil actions in the courts. The only general body established for privacy protection in Australia is the Privacy Committee of New South Wales. That body works, very largely, by procedures of conciliation, negotiation and persuasion. There is no doubt that the Committee has done extremely valuable work. A measure of the importance of privacy protection in the public's mind can be found in the rapid growth of the Committee's business. Every year, the numbers of complaints made to the Privacy Committee increase significantly. The Committee aggregates its experience from dealing with these complaints. In consultation with those affected, it prepares guidelines for voluntary adoption. It has no powers of enforcing the guidelines. It has no means of awarding compensation to those whose privacy is invaded.

The machinery for privacy protection proposed by the Australian Law Reform Commission draws on this local and overseas experience. It starts with establishing the proposition that present Australian law does not provide adequate protection for privacy. In particular its protections to the privacy of personal information are shown to be piecemeal and inadequate. The advent of computerisation linked to telecommunications poses identified new dangers, making the provision of new protections by the law both necessary and urgent.

The Australian Law Reform Commission has published a discussion paper with tentative proposals for privacy legislation in Australia. It sets for itself the task both of establishing certain general principles which should be observed in the collection, use, disclosure and storage of personal information and the enactment of legal machinery which will elaborate those general rules, provide conciliation and mediation in particular cases, permit the development of community awareness about the importance of privacy, facilitate on going law reform and, above all, provide for the just resolution of disputes and the enforcement of fair information practices. Rejecting a number of overseas models, the discussion paper makes it plain that Australia's Federal Privacy Act:

- Should not be confined to computerised information systems.

- Nor should it be restricted solely to Federal public sector (as is still largely the case in Canada and the United States).

. Nor should it be limited in its application to citizens and permanent residents. All persons in Australia should have the protection of these uniquely modern legal rights.

The discussion paper lists various principles concerning the collection, use and disclosure of personal information, its storage and security. It adopts, as a central provision the following 'basic rule' for individual access and challenge.

> The individual should normally be entitled to find out what information is held about him and to challenge it upon specified basis, in appropriate circumstances.

Much of the discussion paper is devoted to spelling out this general statement. Exceptions must be identified. The precise rights of 'challenge' must be clarified. The circumstances in which challenge will be appropriate and the consequences of such challenge must be clarified. The way in which challenge can be used in the first place and turned to an effective defender of the individual and his control over information about himself, must all be explored.

In addition to these general rules a number of specific topics are dealt with in the discussion paper. I can do no more hear than to list them. They include:

* the rules that should govern 'blacklisting';
* the rules that should govern 'matching';
* when 'logging' of access to personal information should be required;
* when 'culling' of out-dated personal information should be necessary;
* when destruction, de-identification or archiving are appropriate to protect individual privacy of personal information.

NEW PROTECTIVE BODIES

The proposals of the Law Reform Commission suggest the creation of three new protective bodies. These need not be expensive proposals. Apart from the first (the Privacy Commissioner), it is envisaged that other bodies would be made up of part-time personnel. The Ombudsmen and the Privacy Committee have demonstrated how much can be done with a small effective staff.

* Privacy Commissioner. A new Federal officer who should handle complaints and conciliate grievances about invasions of privacy and fair personal information practices in the Federal sphere in Australia.

* Privacy Council. A new national body should be established to develop detailed standards for particular forms of personal information systems and for particular information practices which pose special dangers for privacy. The functions of setting standards and handling complaints should be separated. The Privacy Council should:

  - develop codes of practice;
  - elaborate the standards to be observed;
  - give advice on information practices, promote community awareness about the importance of respecting individual privacy; and
  - suggest reform of the law, where this is indicated by advanced in technology or by the accumulation of knowledge and experience.

  The Privacy Commissioner should be a member of the Australian Privacy Council.

* Ministerial Council. Because of the desirability in securing common standards for privacy protection and compatible machinery for the enforcement of those standards throughout Australia, a Ministerial Council should be created of Federal and State Ministers concemed with information practices in their respective jurisdictions. The Law Reform Commission has suggested that, to promote the widespread implementation of uniform, national fair information practices in relation to personal information, Federal legislation should apply not only to the Australian Public Service and throughout the Commonwealth's Territories but also, within the States, to the extent to which personal information may be transmitted between data bases by telecommunications. The Commission has invited submissions on whether the Commonwealth's constitutional powers to legislate on telecommunications could or should be used as a means of securing a single national code of fair information practices in respect of data bases linked by telecommunications. Obviously, this question has political as well as legal and technological implications. But the spectre of disparate privacy protection laws in different parts of Australia is one which practical law makers may have to face up to and avoid. It is a matter which should be of concern to this conference and to all users of computer equipment and programs. How difficult it will be for them if, using instantaneous technology, they must somewhow, in different States, comply with differing legal standards.

REMEDIES IN THE COURTS

In the United States, the Privacy Act may be enforced by the citizen bring a suit in a Federal Court, claiming money damages for non-compliance with its terms, for example refusal to grant access to personal data within the time specified. In Australia, a controversy has surrounded the extent to which a general right to privacy should be created, enforceable in the courts. The good work of the New South Wales Privacy Committee in dealing with hundreds of complaints, indicates what can be done by a 'low key' accessible body which avoids the costs and delays of the courts. Is more needed?

The Law Reform Commission has suggested that it would be desirable to supplement the administrative remedies provided by the proposed Federal Privacy Commissioner. It has suggested that a new civil remedy should be created, enforceable in the courts, for loss, damage, embarassment annoyance or distress caused by breach of the specific standards laid down in the Privacy Act or subsequently established, according to law, by the Privacy Council. It has suggested that money damages should be recoverable in respect of any actual loss suffered by a person as a result of the breach of fair information practices in respect of personal information about him. A number of reasons are given for going beyond the conciliation/mediation model of the N.S.W. Committee. They include, in the Federal sphere, certain constitutional complications. But even more important is the need to keep the remedies for privacy bright, by the actions of the ordinary courts of the land, versed in the protection of liberty, independent of the Executive Government and able to provide remedies and sanctions, civil and criminal, which cannot be given by an administrative agency alone. The need to provide a power of injunction, or the making of declarations of legal rights and the need to provide criminal offences for deliberate or reckless breaches of standards of privacy protection, all necessitate a role for the courts, in addition to the administrative agencies proposed.

Because of the nature of the complaint and reasons of cost, speed and accessibility, it is likely that most claims for privacy protection would be dealt with by the Privacy Commissioner. The very nature of privacy invasions makes it likely that actions in the courts will be rare, because of the publicity usually involved. Access to the courts may be prohibitively expensive for many middle class Australians. The possibility of the Privacy Commissioner being authorised (with the consent of the individual) to take proceedings in the courts is being examined. There may be merit in ensuring that the courts, with their unique remedies and powers and their independence from external pressure should come to play a role in defending the individual in this modern, but vital, attribute of individual liberty.

IS IT ALL NECESSARY?

The discussion so far has proceeded on a somewhat theoretical basis. But the challenge to privacy and individual liberties is anything but theoretical. The discussion paper published by the Law Reform Commission instances many cases where personal information has been used unfairly to the individual. Many more instances are collected in the annual reports of the Privacy Committee of New South Wales. Many cases have simply not come to notice. Other cases or potential cases are not difficult to imagine. Take a few examples:

* Wrong Credit Reference. Mr and Mrs X applied to a finance company for credit to buy a panel van. Their application was initially rejected on the basis of their credit rating. Investigation revealed that Mr and Mrs X had a bad credit record with two credit bureaux. Each bureau had misrecorded credit information concerning Mr X's father against Mr X's name. Both persons lived in the same street, but at a different address.

* Inquisitive Restaurateur. The operator of a chain of restaurants asked all applicants for employment if they had criminal records. Inquiry was made just in case the applicant might then, or at a subsequent stage, be considered for a managerial position. A manager had to obtain a liquor licence, for which a conviction of a serious offence might constitute a bar. After investigation by the Privacy Committee, the company agreed to delete the question from the form. Even if rephrased, it would have been relevant only to applications for a managerial position.

* Incomplete Criminal Record. In 1953 A was charged with committing an offence of offensive behaviour. The charge was dismissed. In 1974 A applied to B for a job. For the purpose of the application, A made a statutory declaration to the effect that he had never been convicted of a criminal offence. B lawfully obtained what was supposed to be a true copy of A's criminal record. But the record was incomplete. In relation to the 1953 charge, it did not say whether A had been convicted or not. Because of the record, A did not get the job and B would not tell him why.

* Threat of Suicide. A journalist who had received a letter from a pensioner who was threatening to commit suicide, sought to secure the pensioner's address from the Department of Social Security. The pensioner had a history of long and severe illness and had been seen from time to time by social workers. Access to the address was approved in this case.

* Police and Legal Records. In July 1978 it was reported that documents of a police crime intelligence unit marked 'strictly confidential' were found at a local garbage dump. One record was reported to refer to a man as a 'potential police killer'. Security in respect of the records had not been properly maintained. In a similar case a printout of confidential records from a solicitor's office turned up in an infants school being used as spare paper for drawing and painting by the school children.

At present, in Australia, there is usually no accessible legal machinery for dealing with cases such as these. Only in New South Wales does a privacy 'watch dog' exist. But its powers do not extend to enforcement of its advice or the provision of damages or other court-like remedies. The growing accumulation of personal information on all of us, both in the public and private sectors, makes it important that new sanctions and remedies should be developed. It is important that sensitive legal machinery should be developed now, so that hand in hand with technological developments, we can develop effective sanctions and remedies which provide the individual with effective means to defend his privacy. Furthermore such laws should provide the record-keeper with clear guidance as to acceptable and unacceptable information practices.

In a world of fast moving science and technology, slow moving lawmakers find it difficult to cope. In the dazzling advances of information science lie many dangers for the individual. A world in which telephones were regularly tapped, individuals were constantly the subject of electronic eavesdropping, optical surveillance was maintained regularly on individual conduct and the information gathered was fed into data bases regularly available to a controlling class seems fantastic. But it is, or shortly will be, technologically perfectly possible. Ultimately, technology exists to serve humanity. It is for humanity to state the terms upon which technology may be used in society. A modern French philosopher, having experienced the War time occupation, said wrily that 'the mere fact that it is a dictatorship of dossiers and not a dictatorship of hobnail boots, does not make it any less a dictatorship'. It is this truism which rings the bell to warn countries such as Australia about the dangers to liberty which may arise from the new information technology, if we nothing. There is a common resolve in Western Europe, North America and Australasia to respond. The response should not be seen as simply the provision of machinery to ensure that information systems are relevant and efficient. There is something more at stake. What is at stake is the role of the individual in the society of the future. The new technology both creates the problem and provides facilities for the solutions. The Law Reform Commission's proposals for new privacy protection in Australia should command the attention of all those in this country concerned about the future of individual freedom in it. Information privacy is a thoroughly modern aspect of freedom.

PUBLIC HEARINGS AND CONSULTATIONS

The Federal Government is committed to the introduction of privacy legislation in Australia, when it has considered the report of the Law Reform Commission. Already legislation has been enacted or is before Parliament which facilitates the access of the individual to certain government information about him. The most important of this legislation is the Freedom of Information Bill 1981, still before Parliament. The proposals stated above are a natural extension of and companion for this legislation. They fit well into the international pattern which is emerging in countries with political and economic systems similar to our own. Greater urgency is undoubtedly felt in the countries of Europe which saw the damage that could be done by the misuse of personal data during the last War. Though the urgency is not yet so plain to Australians, the potential danger is a common one.

The whole point of referring a matter of such sensitivity and complexity as this to the Law Reform Commission is to promote a national debate and the thorough consideration of proposals, before they are presented in a final legislative form. The suggestions of the Law Reform Commission on privacy protection have been put forward in a discussion paper, precisely to promote discussion. Throughout Australia, public hearings have been held by the Commission to secure reactions to the discussion paper by government and business groups, experts and ordinary citizens. To coincide with these public hearings, a series of seminars involving information users was held, sponsored by the Australian Computer Society. Anyone still interested to comment on the proposals for new privacy legislation is invited to secure copy of the discussion papers and to make their comments within the next month

The computer must remain an extension of us. It will be a sad world if humanity becomes an extension of the computer, not the computer an extension of humanity. Deciding where the undoubted values of information flows end and where the legitimate right to respect for individual privacy begins is a difficult task. It requires sensitive judgment in tune with the values of our society. If there is no defender for privacy, fair information practices will rest on flimsy foundations. In the age of computications, we must do more. The new technology requires new legal responses. For 'information privacy' read 'individual liberty'.

Further Information. Copies of the Australian Law Reform Commission's discussion papers Privacy and Intrusions (DP 13) and Privacy and Personal Information (DP 14) are available free of charge to persons prepared to comment on them. For copies write to: The Secretary, Australian Law Reform Commission, G.P.O. Box 3708, Sydney 2001 N.S.W. Australia, Telephone: (02) 2311733. The Commission hopes to complete its report on privacy by the end of 1981 and to report to the Federal Attorney General and Parliament early in 1982.