

THE PROTECTION OF PERSONAL INFORMATION - PRIVACY  
LAWS AND OECD GUIDELINES

Department of Justice, Canada: National Forum on Access  
to Information and Privacy

Ottawa 7 March 1986

"ACCESS TO INFORMATION & PRIVACY - THE TEN INFORMATIONAL  
COMMANDMENTS"



## *Access to Information and Privacy: The Ten Information Commandments*

by M.D. KIRBY\*

### The New "Marxism"

Recently, as light relief to Archbold's *Criminal Pleadings* and Dicey's *Law of the Constitution*, I was reading the writings of Marx. Not Karl; but Garry Marx, a New York academic. Asserting that popular culture, and hit tunes, can sometimes convey, even subliminally, important political and social messages, Marx took as an illustration the hit song of the pop group The Police. Hidden away in the words, he said, was a timely warning to the younger generation of the dangers of the new information technology. The song is "Every Breath You Take." Here is Marx's analysis:

Every breath you take [breath analyser]  
 Every move you make [motion detector]  
 Every bond you break [polygraph-lie detector]  
 Every step you take [electronic anklet]  
 Every single day [continuous monitoring]  
 Every word you say [bugs, wire taps, mikes]  
 Every night you stay ... [light amplifier]  
 Every vow you break ... [voice stress analysis]  
 Every smile you fake [brain wave analysis]  
 Every claim you stake ... [computer matching]  
*I'll be watching you* [video surveillance].

Marx's thesis is as frightening as it is simple. We stand at the brink of remarkable developments in the thriving new technology of informatics both in the public and private sectors. Some of the developments are regulated by current law. Many of them are outside. Computers may match the hundreds of profiles built up on all of us. In the last decade, there has been a massive increase in the ability to collect and process intrusive information about all of us which, but a few years ago, would have been regarded as utterly

\* An earlier version of this paper was presented to the National Forum on Access to Information and Privacy Conference, Ottawa, March 1986. Versions of the paper have also appeared in *Law/Technology Journal* 19 (Winter 1986) and *Computer Law* 2, no. 5 (April 1986).

© All rights reserved. *Archivaria* 23 (Winter 1986-87)

private and totally inaccessible — even to the most powerful government official or corporate enterprise.<sup>1</sup>

Satellites can spot a car or person from 30,000 feet up. They have been used for surveillance of drug traffickers. Light amplifiers, developed for the Vietnam war, can be used with a variety of cameras and binoculars to intrude into the private moment. National security agencies monitor hundreds of telephones. The Hong Kong government is testing an electronic system for monitoring where, when, and how fast a car is driven. A small radio receiver in the car picks up low frequency signals from wire loops set into the street. It then transmits back to a central authority the car's identification number. The system was proposed as an efficient means for the relatively innocent task of checking the payment of road tax in the congested traffic areas of Victoria Island. But what a boon it provides, or would provide, for continuous monitoring and surveillance.

This is not alarmist talk. The features of the new information technology which endanger the value of individual privacy are now well known. According to Marx, the dangers derive from the following features of the technology in particular:

- It transcends distance, darkness and physical barriers.
- It transcends time, because of the capacity to collect and store massive amounts of data which can be retrieved whenever needed.
- It is capital- rather than labour-intensive, because it is no longer necessary to have human intervention. The computer can analyse all.
- It is universal in its application, decentralised and triggers self-activating policing.
- It has low visibility or even total invisibility.
- It grows ever more extensive and covers larger areas of life, ever more deeply.

These are trite statements about a pervasive technology which is overwhelmingly beneficial in its potential to release mankind from the millstones of routine and mindless drudgery. However, a poll conducted in 1985 by Louis Harris-France in eight industrial countries indicates that "invasion of privacy and unemployment continue to be viewed as two significant consequences of data processing."<sup>2</sup> In the United States, 68 per cent of those polled agreed that it would be increasingly possible to use computer data banks to infringe personal privacy. Knowledgeable people, who are not Luddites, recognize that a hitherto important feature of our form of society is seriously endangered by what is otherwise a beneficial technological development. Moreover, it is a development which has distinctly positive features for the enhancement of freedom. For example, the new information technology promises the improvement in cost effective access to official information. In this way the public accountability of politicians and bureaucrats may be increased so that they extend far beyond the occasional visit to the ballot box which was previously the theoretical occasion for enforcing the ultimate accountability of the Executive Government to the People.

<sup>1</sup> Garry Marx, "I'll Be Watching You," in *Dissent* (Winter 1985).

<sup>2</sup> T. Riley, "Privacy in the 1980s — Another Trade Barrier?" *Journal of Commerce* (17 October 1985), p. 1.

In all advanced English-speaking democracies three changes have occurred which promote the demand for privacy and freedom of information (FOI) laws. These are:

- I The significant growth in the role of the public sector, precipitated by the urgent needs of the Second World War and continued and expanded ever since. This phenomenon, and the vast panoply of agencies and officialdom thereby created, demolished many of the vestiges of the mythology of ministerial accountability. It has led to a rational insistence upon new institutions and rights which translate theoretical accountability into daily practice.<sup>3</sup>
- II The general advances in the education of the community has had a dual impact. First, it has created an ever-expanding pool of well-informed citizens, impatient with the paternalistic notion that administrators necessarily know best. Secondly, it created, particularly in the educated middle class, a group of people willing to utilize new rights and to enforce them in the courts and in the protective administration agencies set up.
- III Then came the new technology itself. As Marx and others have demonstrated, it presented novel problems, problems of data protection and data security. But it also presented potential solutions. Keys, passwords and encryptions could be introduced to bar access to personal information, even to an inquisitive civil servant who, in the old days, might have had access to paper files. On-line facilities could assure the data subject, potentially, of the right of access to data about himself or herself, in a way that the inefficiency of the old systems could not necessarily ensure.

Thus, the issue in a nutshell is one of thinking, as the Americans say, "positive." Taking advantage of the remarkable and pervasive technology of informatics whilst, at the same time, acting with resolution to defend elements of individual privacy, deemed important for the liberty of mankind in the future — a future likely to be increasingly pervaded by the technology of informatics.

#### The Thread of Ariadne

The past decade or so has seen important legislative responses to informatics in all of the advanced English speaking democracies. Freedom of information and privacy laws have been enacted in the United States and Canada.<sup>4</sup> Privacy legislation has been enacted in the United Kingdom. But, although 57 per cent of the British people last year told an opinion poll that they thought FOI would help protection of rights "a great deal,"<sup>5</sup> the United Kingdom government seems to adhere to the old mythology of ministerial accountability, the Official Secrets Act and the world of "leaks" which tends to accompany, nowadays, regimes of too much secrecy. The Ponting trial<sup>6</sup> and the Westland helicopter affair both show what happens in secretive administrations in the age of the photocopier.

3 L.J. Curtis, "Administrative Law Reform — Impact on Public Sector Management," unpublished paper for the National Government Accounting Convention, University of Adelaide, 21 February 1985.

4 United States, *Freedom of Information Act*, 50 U.S.C. 552; Canada, *Access to Information Act*, 1983; Canada, *Privacy Act*, 1983.

5 P. Kellner, "All so Wrong about Rights," *Times* (London), 1 July 1985.

6 Reported in *The Economist*, 16 February 1985.

New Zealand has enacted a FOI law.<sup>7</sup> And when I was there in 1986, that country was looking at reform of that law and at the enactment of privacy legislation.<sup>8</sup> In Australia, a Freedom of Information Act was enacted by Federal Parliament in 1982. It contained an important section for rights of access to personal information and for the protection of private information. Comprehensive federal privacy laws have been promised.<sup>9</sup> But hand in hand with these developments comes a proposal for a national identity card to co-ordinate federal data banks as a suggested means of combating tax and social security fraud.<sup>10</sup>

Recently, I had to offer a Foreword to a forthcoming publication, to be printed in Canada, on the problems and prospects of these information laws.<sup>11</sup> Upon looking through the reports of two of the contributors, Ms Inger Hansen and Dr. Harold Relyea, and the report of the Australian legislation offered by Senator Alan Missen, it became clear that a number of common themes were emerging. They chart the way ahead for those concerned about information law in the last decade of the twentieth century. With differing emphasis, the authors call attention to concerns which will clearly affect the law and administrative practices involved in the exercise of privacy and FOI rights for years to come.

Hansen and Relyea stress the concern in Canada and the United States that FOI is being used (or abused) to breach the legitimate expectations of business confidentiality. This confidentiality may sometimes be undermined by the revelation, pursuant to FOI law, of information supplied by business (usually under compulsion) to the government. How are these competing rights to be reconciled and the integrity of FOI maintained, whilst ensuring legitimate claims to business secrecy and candid supply of business data to government?

Concern is also expressed in Canada and the United States about the use of FOI to undermine, frustrate and delay the processes of law enforcement. Particular anxiety is felt about the so-called "mosaic" phenomenon — as a result of which, even where identifiers have been deleted, some material supplied pursuant to FOI can assist anti-social persons to identify public informers or to secure other information which public policy suggests should be kept secret.

Concern about cost of FOI is a theme running through all reports on the operation of information legislation. There is the suggestion that this is a luxury which, however desirable in principle, our communities simply cannot afford. There is also the suggestion that, depending as it does on the activities of enthusiastic individuals, our FOI and privacy laws are very much guardians of the educated middle class. They provide little in the way of enhanced freedom for those people who are most dependent on, and under the surveillance of, government — the social security recipients, veterans, hospital patients and others whose very position of dependence often makes the enforcement of their information rights a matter of theory rather than practice.

7 New Zealand, *Official Information Act*, 1982.

8 Cf. J. Eagles and M. Taggart, *Report on Reform of Official Information Act 1982* prepared at the direction of the Hon. G.W.R. Palmer, Minister of Justice and Attorney-General, mimeograph, October 1984.

9 Australia, *Freedom of Information Act*, 1982 ss 11, 49. See G.J. Evans, *Commonwealth Record* 9 (1984), p. 2537.

10 Australia, Department of Health, *Towards Fairness and Equity: The Australia Card Program*, 1986.

11 T. Riley, ed., *Access to Government Documents: Some International Perspectives and Trends*, forthcoming.

In Australia, the concern about FOI and privacy laws has changed in the last decade. From the early debates about the numerous exemptions and conclusive ministerial certificates under the FOI Act, the concern today has shifted. So few ministerial exemptions have been claimed that the battle ground has moved. Now, the counter-reformation comes from the bureaucrats who point repeatedly to the cumbersome and costly machinery to which they must devote scarce resources. And those concerned about spreading the impact of FOI and privacy access rights point to the narrow usage of those rights, the widespread ignorance about them, their substantial confinement to the educated middle class and the retreat from earlier public campaigns to promote general knowledge by media advertising, pamphlets and the like.<sup>12</sup>

At this level of the debate, it would be possible to trace a thread of Ariadne through the controversies. Common themes undoubtedly exist. There is some evidence of a counter-reformation, as attention is laid by bureaucrats and politicians in many lands, upon cost and the various problems which the first decade of information legislation has disclosed.

Instead of taking this course, I have decided, with due modesty, to propound the ten information commandments. It was said of President Wilson's fourteen points that he had divined four more than the Almighty. Being a more diffident type I have preferred to follow the Mosaic tradition. Hence the ten information commandments which will doubtless, in due course, be known as the Ten Information Commandments of Ottawa.

### The Ten Information Commandments

#### *I Contemporary technological developments endanger human rights and civil liberties and require responses from society — including the legal system.*

This first "commandment" states the obvious. It is not confined to informatics. The most remarkable feature of the late twentieth century is the coincidence, at one moment of history, of three important technological developments. I refer to nuclear fission, biotechnology and informatics. Each of these developments has implications for human rights and civic freedoms. Information technology presents problems, some of which have been identified already by Garry Marx. Biotechnology presents quandries which go to the very definition of human life itself. Human cloning, *in vitro* fertilization, the growing of human body parts and numerous other features of genetic engineering and biotechnology present major dilemmas to the philosopher, the lawyer and the law maker. In the Australian Parliament in 1986, a Parliamentary committee examined a Private Member's Bill designed to restrict and control many biotechnological developments, in some of which Australian scientists have made notable contributions.<sup>13</sup> Of nuclear fission, I need say nothing — except that, unless the international community can bring this technology under effective international control, the long run prospects of mankind's surviving accident, mistake or nuclear folly appear problematical. So the starting point — the beginning of wisdom — is a realization of the enormous challenge which technology presents to humanity in our generation. We need a Luther of jurisprudence to lead us to the legal solutions and political leaders of wisdom to lead our communities thoughtfully to the responses that preserve life and freedom.

<sup>12</sup> Australia, Attorney-General's Department, *Freedom of Information Act, 1982*: Australian Government Publishing Service, *Annual Report 1983-84, 1985*, pp. 107-9.

<sup>13</sup> Australia, *Human Experimentation Bill, 1985*.

*II The fertile common law system, even as enhanced in some countries by constitutional rights, is insufficient to provide adequate responses to the challenges of technology. Legislation is needed.*

There are some people who say that the common law, developed by the judges, will be as adequate to defend our liberties in the future as it has in the past. No doubt there is a role for the common law. It must surely respond to technological change. Benjamin Cardozo once said that the law, like the traveller, must prepare for the morrow. In the United States, with the famous language of the Bill of Rights and in Canada with the Charter of Rights and Freedoms, a scope is offered to the judiciary to enhance the creative element which has always existed in the common law. But even in such countries, and even more so in countries such as my own, without such a catalyst for judicial creativity in the protection of rights in the modern era, more will be needed. The High Court of Australia recently reversed a decision in which I had participated. It was a decision relevant to information rights. The Court of Appeal had declared that, in modern circumstances, the common law of natural justice required the giving of reasons by public officials enjoying legislative discretions.<sup>14</sup> The High Court, referring to old authorities, many of them preceding the three developments to which I have referred, unanimously ruled that a right to reasons was not required by the rules of natural justice.<sup>15</sup> Development of the law here, it was said, was for the Parliament, not the courts. A signal was sent out cautioning against judicial creativity. It was said that in other countries of the common law, for example India, where a right to reasons is now established, constitutional considerations, in the form of fundamental rights, might explain and justify developments in the law. Perhaps the law in Canada will respond more readily to changing times and changing technology because of the facility provided by the Charter of Rights and Freedoms. But in Australia, as in New Zealand, England and elsewhere, the judiciary since the nineteenth century and the reforms of Parliament has, with notable exceptions, preferred to emphasize the non-creative features of the common law. Yet the signal that calls for judicial restraint calls equally for legislative attention, in default of which the judges will be urged to remedy wrongs and to provide defences to freedom.

*III In some cases, the technology itself demands or even produces legal reform.*

This third rule refers to the tendency of modern technology to undermine current law or to render it irrelevant or ineffective. I have already mentioned the way in which the photocopier undermines excessive secrecy. Doubtless this is why photocopiers are kept under lock and key in the Soviet Union. The technology of photographic reproduction and on line linkages reduces the capacity to keep things secret. The self same technology that presents the problems of privacy promotes the flow of information that tends to enhance accountability both in the public and private sectors. But in the field of informatics, the results can be surprising. One case is well known and is called to attention by Professor Jon Bing of Norway. A social scientist in Norway sought on-line access, under United States FOI law, to NATO deployments in Norway. Such information was a state

<sup>14</sup> *Osmond v Public Service Board of New South Wales* in *New South Wales Law Report* 3 (1984), p. 447; *Law Reports of the Commonwealth of Nations (Constitutional)* (1985), p. 1041.

<sup>15</sup> *Public Service Board of New South Wales v Osmond*, unreported, High Court of Australia, 21 February 1986.

secret under Norwegian law. The social scientist was prosecuted in Norway. Information technology, with its international applications reduces, by transborder data flow, the effective operation of the sovereign laws of domestic jurisdiction.<sup>16</sup>

*IV The People are not always the best judges of their own interests. Informed observers have a duty to identify dangers to freedom.*

One of the chief arguments which the minister proposing the national identity card in Australia continually refers to is that public opinion polls show that nearly 70 percent of Australians favour a national identity card with photograph.<sup>17</sup> In a democracy, it is natural for intellectuals to bow to the corporate wisdom of the People. If the people want an ID card, why should they be denied such a facility? Especially if it would help combat welfare and tax fraud? The answer, sadly, is that the public is all too frequently willing to participate in the destruction or erosion of its own liberties. It is to informed people (particularly lawyers conscious of our long constitutional history and the famous struggles for freedom) that there falls the sometimes unpopular function of holding out against the popular tide. Opinion polls may persistently favour the reintroduction of the death penalty. They may favour the return of flogging and, who knows, even transportation to a far-off place, such as Australia. But such opinions may be based upon false impressions or ignorance of the available data. They may ignore the statistics that show the ineffectiveness of such punishments. They may ignore the statistics that show the fall in jury convictions where capital punishment is available. They may be based on ignorance of the counter-vailing effects of such punishments.

So it may be with a national identity card. It may be based on a desire of people without access to gold American Express cards to have a nice plastic card, as other people have. It might be based on the notion that "if you have nothing to hide," the card can do no harm. It might conjure up the memory of the occasion when proof of identity would have been useful. But it remains for those who are aware of the special relationship that exists in countries of the common law between authority and the citizen to point to the dangers. A dentist who survived Auschwitz may declare that the best thing about living in Australia (it could equally be Canada, the United States or England) is that he is never liable to be stopped on the corner by someone in uniform with the demand "Papierenii!" Yet provide an ID card and the risk exists that the data base will be enhanced and that more and more officials will seek access to it, in the name of efficiency. And that in due course carrying the card will be obligatory. And producing it will become a commonplace and, ultimately, in response to some outrage, obligatory. In the space of a few years, an important principle that marks off the intrusion of officialdom into our lives could be demolished. And the intrusion might not just be physical. It might go on behind the scenes; intrusion into the data profile where more and more decisions affecting the subject may be made without the knowledge of the data subject.

Lulled by a trivializing diet of soap operas, cowboy Westerns and Manhattan gun battles, people become indifferent spectators to or even conspirators in the erosion of their own freedoms. Should we care? Should we who are aware of the long battles for freedom also surrender — acknowledging that some erosion of privacy is inevitable as a product of

16 J. Bing, P. Forsberg and E. Nygaard, "Legal Problems Related to Transborder Data Flows: An Exploration," mimeographed (Organization for Economic Cooperation and Development, 1983), p. 59 ff.

17 N. Blewett, news release, Canberra, 10 February 1986.



the new information technology? The Fourth Commandment teaches that we *should* care. And that it is the responsibility of politicians, and those who advise them, to work, even in the face of popular indifference or opposition, for the preservation of hard-won freedoms. For once they are lost they are rarely regained.

*V The costs of information rights must be counted. But so must the intangible benefits.*

In the jargon of the economist, it is important for lawyers who talk of liberty and freedom, to take into account the incremental costs involved in the externalities to decision making. The protection of freedom and the assurance of fairness have a cost. It involves the assignment of scarce resources. The recent *Singh* decision in Canada, obliging hearings for refugee immigrants was a blow for administrative fairness. But clearly the cost of providing this facility will run into millions of dollars. The provision of the facility to the persons affected will necessarily result in the denial of benefits to others. That is the simple consequence of the economic problem.<sup>18</sup>

So it is in information rights. There is now a great deal of talk, particularly in Australia, concerning the costs of FOI and privacy rights. There is a similar debate in the United States. But whereas the American FOI legislation is now a robust adolescent, the same cannot be said of the equivalent laws in Canada, Australia and New Zealand. The combination of talk about cost of the provision of information rights, the inevitable concern by politicians about skeletons they would rather leave in the computer cupboard, and the hankering of not a few public servants for a return to the "good old days," all present the danger of the Information Counter-Reformation. It is a danger which supporters of information rights must repell. They must work with special vigour in countries such as Canada and Australia because of the relative ease with which governments, dominating the legislature, could secure the rolling back of legislative entitlements to information — whether public or personal. The rolling back of such rights can be done by frank legislative amendment and repeal. But it can also be done, in practice, by the introduction of or increase in charges. These may effectively bar some of the more deserving people from exercising their rights. Or it can be done by cutting back in publicity about the existence of the rights, so that they remain (in practice) the province of the media, of corporations and of educated middle class citizens.

It is natural that in more difficult economic times governments should be concerned about the costs of information rights. The direct costs include not only the administrative staffs and bureaucratic time. To them must be added the provision of court rooms, judges and tribunal members, shorthand writers and so on. As well, there are the opportunity costs — the other facilities and benefits foregone by virtue of the decision to stick with information rights.

These concerns have led government ministers, and the Leader of the Opposition, in Australia to foreshadow the possible winding back or limitation of review mechanisms for the enforcement of information rights.<sup>19</sup> This is sure to be an important issue in the

18 M. Bouchard, "Administrative Law in the Real World: A Canadian Perspective," unpublished paper presented to the New Zealand Legal Research Foundation Seminar on Judicial Review of Administrative Action, Auckland, February 1986.

19 See, for example, Senator P. Walsh, Minister of Finance, in Australia, Senate, *Commonwealth Parliamentary Debates*, 17 April 1985; J. Howard (Opposition Leader) in address shortly after election as Leader of Opposition.

decade ahead. It may be that corporations and others who are major users of such rights should pay a differential fee in recognition of the fact that they can pass such business expenses on to consumers using their products. It may also be that attention needs to be given to the more cost-effective way of delivering information: avoiding the cumbersome, expensive and dilatory machinery of courts and tribunals. But when the public costs are added up, so must the public benefits. And the relativities must be considered. They include the well known statistics that the cost of FOI in the United States is less than the upkeep of lawns on golf courses for overseas defence personnel. And as Dr. Relyea points out, against the cost of providing information that people want to know must be considered the cost of official government information services that nowadays pour out thinly disguised propaganda, repeated through media handouts, concerning what the government *wants* people to know. The former may be a healthy corrective, on occasion, to the latter.

*VI Information laws must be developed flexibly because of changing technology and the rapidly changing perceptions of the problems.*

Not to devise and implement privacy laws, in the inadequacy of the common law and current legislation, is to make a decision. It is to stand quietly by whilst the technology itself erodes hitherto valued rights. But the counterpart of this principle is that inflexible laws can outlive the understanding of the problem they have been introduced to solve. This is why Professor Simitis has said that the data protection laws are now at a "turning point." An illustration of this truism can be given. Many of the laws already put in place rely heavily on the right of individual access as a means of protecting individual privacy rights. But the effective utilization of this most beneficial right depends upon large assumptions. It depends upon knowledge by the individual that there is something to be concerned about. If there is no notification that you are in the system, decisions may be made, vital to your life, and yet you may be blissfully ignorant. Similarly, the right of access makes large assumptions about individual initiative and enthusiasm. Realism might well raise different considerations. Apathy, resignation or a feeling of powerlessness may necessitate other solutions, if true data protection is to be afforded beyond the powerful and articulate who exert their rights. There is a tendency in our kind of society to slip into legislative mythology. It is an easy myth to believe that accountability is provided by a right of access and that information rights are thereby protected. In fact such facilities should be seen as the start of a long journey -- not arrival in the Promised Land.

*VII Information rights must extend from the public sector (where they have been developed) to the private sector.*

So far, comprehensive information laws have concentrated on the public sector. This is natural for it is in that sector that critical information affecting all citizens exists. But increasingly important to our lives, and often insusceptible to national control, are large corporations -- including transnational corporations. People in the private sector tend to be foremost in asserting the right of accountability by public officials and access to public data. But the selfsame principle has relevance to the private sector as well. Its full relevance is yet to be worked out. Of course, there is already much accountability by the private sector including in the market. But information rights concern individual power. And power exerted in relation to the corporate state may be equally applicable in relation to dealings with private enterprise. Voluntary guidelines, such as compliance with

the Organization for Economic Cooperation and Development (OECD) privacy principles, may provide a starting point. But it is scarcely likely that this will be adequate in the long term.

*VIII Information technology presents international issues that require international solutions.*

The need for transborder solutions to information rights is self-evident in federations such as Australia, Canada and the United States. But there is a wider international stage. The technology itself is universal. The problems presented necessarily transcend state borders. The OECD Guidelines were developed in the hope of stimulating consistency in legislative and administrative approaches to information rights in the context of privacy. Now, other international agencies are endeavouring to develop rules which can facilitate common approaches. UNESCO has just embarked on a major informatics programme. The Intergovernmental Bureau for Informatics in Rome has established a commission to promote a dialogue on data law and policy between the advanced countries of the OECD and the developing world. The technology must interface. Gross inefficiency will result if legal regulations are enacted which are incompatible and yet must be compiled with transborder flows of data. Data havens may destroy the effectiveness of information rights. The three technological developments of our time — nuclear fission, biotechnology and informatics require of us that we should lift our sights from parochial and purely nationalistic approaches to the law. Until now, law has been very much jurisdiction bound. International technology imposes on us the need for international approaches to legal regulations. We in the developed world must become more conscious of the needs and concerns of those less rich. They follow the caravan of the information economy.

*IX Legal responses to information rights must attend to real problems and not content themselves with myths and mere symbols.*

This principle has already been foreshadowed. The easy thing for law makers to do is to establish a bureaucracy with attractive titles, set up with a fanfare announcing that information is free and privacy is guaranteed. What is important is the fine print. It has always seemed to me that the value of the OECD Guidelines lay chiefly in the formulation of a short list of relatively simple principles for information practices. If these became well known and generally accepted as a Bible of fair information practices, much would be achieved. Sanctions and advisory mechanisms are needed to deal with the problems that arise. Most people at the work place simply require a series of simple rules, ultimately backed up by the law. The simpler the rules are kept and the fewer in number, the more likely it is that fair practices will result. In the field of FOI, rights of access will not promote effective accountability unless they are reinforced by community rights of access to the public media. The concentration of the media in few hands may undermine the effectiveness of official information laws because it prevents vital information flowing through to the community at large. Thus it is the reality of information rights that we should be concerned with, not the mythology. Laws which talk of "the consent of the data subject" sound fine. But to an unemployed pensioner seeking a social security benefit, or a hospital patient seeking treatment or an employee seeking information which does not result in dismissal or destroy advancement prospects, it may sometimes be necessary to go beyond reliance on the courageous individual. Information laws which depend exclusively on

individual motivation for enforcement are much better than nothing. They are a step in the right direction. But they fall a long way short of providing effective protections against all of the implications of the new technology.

*X Democratic values must be preserved and it is at least questionable whether our democratic institutions can adequately respond to the challenges of technology.*

This brings me to my last "commandment." I approach my conclusion on a sombre note. Those who look at the history of Parliamentary democracies in this century may be generally optimistic about the future. Despite many challenges, the institutions have survived. The alternative systems are infinitely less flexible and uniformly more oppressive. But the problem for Parliamentary institutions, posed by rapid technological change, is that of keeping pace. If nothing is done, a decision is made. Yet the very technicality of the changes make it difficult for the lay politician (and indeed those advising him or her) to comprehend all of the ramifications. Furthermore, many of the changes are highly controversial, as debates about the privacy of children against their parents and debates about biotechnological experiments clearly demonstrate.

In the face of such complexity and controversy, there is a natural tendency to Parliamentary inaction. It is understandable. But it is dangerous. It is especially dangerous if it coincides with the disinclination of the judges (themselves often scientifically illiterate) to mobilize the creative machinery of the common law. There are, at least, some signs that this is what is occurring. It is most likely to occur if the Executive, which dominates Parliament, loses enthusiasm for information rights. That loss of enthusiasm may be dressed up in the name of economy and cost/benefit analysis. But it may simply disguise age old issues of power: where is power to lie? In Australia, there is much evidence of the institutional incapacity to respond. Only one state (Victoria) has enacted an FOI law. In others it is repeatedly promised, but nothing comes of the promises. Only one state (New South Wales) has a general privacy law and that is of limited effectiveness. The federal privacy law is a long time coming. And there is much more vigour in pressing on with a national identity card, despite the dangers it poses for privacy than in embracing privacy protection laws, limited as they may be. In the field of information rights, public lethargy now conspires with unsympathetic noises both from Government and Opposition quarters.

#### Conclusions

What is the result of this analysis? Is it that late twentieth century man and woman, lulled in the global village into an intellectual haze by a constant diet of media trivia, have lost concern about political accountability? Or are indifferent to (and even conspire in the destruction of) privacy rights? Political accountability becomes a television war between competing electoral jingles — with political parties sold like soap powder to a people programmed to watch personality politics, devoid of concern with the large issues and obsessed by the parochial.

You might say that if 70 per cent of the people want the introduction of the means used in other times and other places to destroy liberty, then governments and politicians must bow to the superior wisdom of the people and their assessment of their information rights.

But that wisdom depends on knowledge. And it is up to those who have the knowledge and can see the problems to act responsibly and courageously. I remain incurably optimistic. But in the darker moments of contemplation, there is a lingering doubt. And even more than its concern about the survival of political accountability and the persistence of privacy in the age of informatics is the institutional concern. In such a time of rapid change, of complex science and of high controversy, can our lawmaking institutions cope? That is the question that transcends even the privacy and freedom of information issues. They are a microcosm of a larger problem. For if our Parliamentary democracies falter here, they admit their incompetence to govern us in the twenty-first century — whose watchword and engine will be science. Accordingly, we must remain optimistic about our capacity to adapt our institutions and laws to rapid technological change. A loss of confidence or heart — and a breach of the Commandment of optimism — is a surrender to the nagging doubt that technology is inherently elitist and autocratic and that democracy, with all its inefficiencies, cannot survive into the twenty-first century. We must make it our business to ensure that this prophecy of gloom proves wrong. But the responsibility for rational optimism is ours.