

# Overview

## Background

Privacy laws have not just sprung up out of nowhere. Privacy has developed from a number of imperatives.

### INTERNATIONAL CONTEXT

There has been a worldwide resurgence of interest in information privacy law since the early 1990s. This is the third period of active international consideration of privacy issues following:

- initial articulation of the right to privacy in the late 1940s;
- detailed standard setting from the late 1970s to the early 1980s.

Most of the present activity arises for reasons of harmonisation within an enlarged European Union, the adoption of human rights in Eastern Europe and fresh examination of the issue by jurisdictions outside Europe.

#### *Human rights origins*

On 10 December 1948 the General Assembly of the United Nations proclaimed the Universal Declaration of Human Rights. This year marks the 50th Anniversary of that historic act. Article 12 of the Universal Declaration provided that:

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

Little attention was paid to states’ observance of the obligation to protect individuals against arbitrary interference with their privacy for the first 20 years of the Universal Declaration. However, in 1966 the right to privacy was incorporated into Article 17 of the International Covenant on Civil and Political Rights. The Covenant introduced two compliance mechanisms. The first is the requirement on states parties periodically to report to the UN Human Rights Committee in relation to compliance with the Covenant. New Zealand has cited the Privacy Act to the Committee in its report on compliance with Article 17.<sup>1</sup> The second is the entitlement of people in states, such as New Zealand, which have ratified the Optional Protocol to take complaints to the Human Rights Committee if their governments have failed to observe the Covenant and no local redress is available. Increasingly, privacy issues have been considered by the Human Rights Committee.

<sup>1</sup> See Ministry of Foreign Affairs and Trade, *Human Rights in New Zealand: Report to the United Nations Human Rights Committee under the International Covenant on Civil and Political Rights*, Information Bulletin No 54, June 1995, paragraphs 84-92.

The human rights approach to privacy issues has also been actively pursued in Europe. The Council of Europe was set up in 1949 with the atrocities experienced across the European continent fresh in states' minds. The Council sought to achieve a greater unity between its members to safeguard individual rights and realise the ideals and principles represented in the common European heritage. The Council's concern with privacy issues dates back to the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950. Article 8(1) of the Convention provided:

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

A number of actions have been taken against European states for breach of that article.

#### *Articulating privacy principles*

General articulation of the right to privacy contained in the human rights instruments could not, of themselves, ensure the protection of privacy given their lack of detail and the challenges to privacy, especially the increasing technological challenges posed by large computer databases.

In 1968 the Council of Europe embarked upon an examination of whether member states' national laws were sufficient to protect personal privacy in the face of modern technology. This led, in the late 1970s, to the drafting by a committee of experts of what was to become the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention No 108”).

Convention No 108 has been hugely influential within Europe. Most member states enacted data protection laws along the lines of the Convention by the mid 1980s. There has been a further wave of data protection laws in the 1990s with the demise of communist regimes in Central and Eastern Europe. The governments and peoples of those countries wanted to embrace human rights standards. The Council of Europe is their prime reference point for privacy and other human rights.

Many of the data protection laws adopted as a result of Convention No 108 are being replaced this year by new laws brought about by the EU Directive on Data Protection. One of the most significant changes is the application of data protection laws to “manual data”. This highlights what has generally been seen as the most significant failing of Convention No 108. By concentrating solely on automatically processed data it failed to address the totality of information privacy.

In the late 1970s the OECD appointed a group of experts on transborder data barriers and privacy protection which was instructed to develop what were to become the OECD Guidelines. This group collaborated with the Council of Europe's experts which helped ensure consistency between the Guidelines and Convention No 108. The OECD Guidelines do not limit their application to automatically processed data and this may ultimately mean that they will be more enduring than Convention No 108. Most OECD states have adopted privacy legislation based upon the OECD Guidelines.

Although the Council of Europe and the OECD together include most of the developed world, their membership does not comprise the majority of the world's nations. The United Nations adopted Guidelines for the Regulation of Computerised Personal Data Files in 1990. These provide governments with a basis upon which they may legislate on privacy consistently with the approach taken in Europe and the OECD. However, the UN has not been active in the area of information privacy and its 1990 Guidelines are not seen as particularly influential. The UN guidelines, in a similar fashion to Convention No 108 a decade earlier, focus upon “computerised” data. In my view, it is no longer sensible to concentrate solely upon computerised data and an approach that covers all personal information, or at least principal categories of “manual data”, is far more appropriate.

*European Union Directive on Data Protection*

The European Union (formerly known as the EC and EEC) only became fully involved with data protection with the issue in 1995 of the Directive on Data Protection which seeks to harmonise the law across a Europe without frontiers. A draft of the Directive was issued by the EC Commission in 1990 with a European Parliament version released in 1992. The release of the draft Directive created a great deal of interest within and beyond the borders of the EU. The main international interest related to transborder data flows and the controls and prohibitions that EU States will be obliged to place on the export of personal data to jurisdictions which do not provide “adequate protection” for the data.

Work had already begun in New Zealand on developing information privacy legislation but undoubtedly the 1990 release of the draft directive spurred action which might otherwise have been delayed. New Zealand was hardly alone in responding to the EU Directive in that manner. Appendix C lists 22 other jurisdictions which have enacted general privacy or data protection laws since 1992. Experience in other similar countries sharing our values and commitment to human rights suggests that New Zealand would eventually have legislated in any case. However, the EU Directive hastened the legislation and meant that it was in the country’s economic interests to be able to show that our law applies “adequate protection” to data received from Europe.

*Relevance of international considerations to the review*

Parliament directed me in section 14(b) and 14(c) to take account of New Zealand’s international obligations, and to consider any developing international guidelines on privacy, when carrying out my functions. International considerations have borne upon my review in a number of ways. For example:

- New Zealand has accepted the OECD Guidelines and it has been necessary to ensure that any proposals for change are consistent with those Guidelines;
- the EU transborder data flow controls which guide European countries raise the prospect of barriers to the transmission of information and it has been desirable to identify and address any shortcomings to “adequate protection” in New Zealand law.

Throughout the report mention is made of the international dimension of the issues under review.

**TECHNOLOGICAL CONTEXT**

This year marks the 50th anniversary of the birth of the first modern computer. In 1948 a team from Manchester University built the world’s first computer with Random Access Memory which it dubbed “baby”. As with the other 1948 event, the Universal Declaration of Human Rights, the development was an outgrowth of Second World War experiences. The war effort had driven significant advances in technology and the pace has since accelerated. Fifty years on the world grapples with the “Y2K” or “millennium bug” problem which threatens to destroy or corrupt certain personal or other data and perhaps ruin businesses and harm individuals in the process. Undoubtedly, the baby has matured. In a single generation the ubiquitous computer has become pivotal to our lives, businesses and economies.

*National and international responses to technology*

By the late 1960s unease had emerged as to the effect that machines and technologies were having, or might have, on individual autonomy and privacy. The particular technological application at the forefront of public concern varies over time but the power of the computer is always central to the concerns. Capacity of computers was understood to be growing exponentially. In the late 1960s and the early 1970s, the focus tended to be upon the large central databases controlled by governments. Orwellian images of an all knowing Big Brother state were frequently mentioned. The fear of data surveillance also tended to merge into civil liberties concerns at law enforcement and state control.

Concern about the technological challenge to privacy posed by large databases was most vividly illustrated in New Zealand by the strong legal controls placed upon the law enforcement database in the Wanganui Computer Centre Act 1976. “Bugging” and “tap-



ping” were also high on the list of technologies raising privacy concerns. In the same period, a series of laws were enacted governing the interception of private communications.

The outcome of the technological concerns in the 1960s and 1970s, and the various legislative responses in developed countries, led to international moves to establish consistent sets of privacy principles. There was a concern that the technological challenges were such that a legislative response in any single country would be ineffective on its own. The Council of Europe Convention No 108 explicitly addressed “automatically processed data”. The OECD, in facing the same challenges at the same time, deliberately developed a set of technology neutral guidelines. The Privacy Act has followed this OECD approach.

The period since the OECD Guidelines and Convention No 108 has seen the common sets of principles applied to a succession of challenges posed by new technologies. There has been debate in the 1990s as to how successful the OECD Guidelines are and whether they are as truly technology neutral as first believed. For example, it is sometimes suggested that the notion of a “data controller” in the OECD Guidelines fits comfortably with 1970s understanding of mainframe computers but is less appropriately applied to distributed systems.

#### *Some local technological issues*

The period since 1993 has seen the introduction, or proposed introduction, of a number of technologies posing challenges for privacy of New Zealanders. For example we have seen the:

- nationwide introduction of caller ID;
- appearance of smartcards;
- commencement of government data matching;
- broad adoption of email for communications;
- rising popularity of the Internet;
- establishment of national sports drug testing;
- unveiling of plans to issue digitised photo ID driver licences;
- prospect of electronic road tolling and the tracking of motor vehicles;
- introduction of various swipe-card retail loyalty schemes;
- construction of CCTV surveillance systems in public places;
- electronic counting of votes;
- computerisation of public registers;
- almost universal adoption of Eftpos in retail outlets.

Some of these proposals have developed with a degree of study and consultation. However, in our rapidly changing technological world this is the exception rather than the rule. New technologies emerge, and existing technologies converge, at a fast pace and the market tends to dictate their adoption. New technologies are rapidly used by businesses and governments if they appear to offer efficiencies. Frequently, privacy is the loser, sometimes in small ways, sometimes in a quantum leap.

It is clear that there will be a host of new technological issues and challenges for privacy in the next five years. Undoubtedly the Internet will be a matter of interest as digital cash comes into use and the debate about access to encryption technology continues. I expect vehicle tracking and electronic road tolls to be a particular matter for study in New Zealand. We will in all likelihood see further convergence of technologies as particular applications are linked to computers directly or via the telecommunications network. We may see extended uses of older privacy-intrusive technologies such as those involving the interception of private communications, CCTV surveillance and drug testing. “Cutting edge” technologies like smart cards and biometric identification may be brought into wider use.

#### *Benefits to privacy of technology*

New technology is not always detrimental to privacy. I hope that ways may be found to

use technological advances for the benefit of individual autonomy instead of always seeing privacy as the loser or accepting some compromise which salvages some vestige of previously enjoyed privacy rights.

There is scope for the adoption of new Privacy Enhancing Technologies (PETs) so as to give individuals the opportunity to participate in anonymous transactions. The creation of transactional data trails in electronic commerce, using individuals' identities, poses a real risk of mass profiling and "dataveillance" to the detriment of individual privacy. I hope that privacy impact assessments of significant new proposals will increasingly identify opportunities for adopting PETs. I have already taken the view that an anonymous option would be vital to any mass electronic road toll proposal.

The wider availability of encryption technology also offers the possibility of enhancing privacy and guaranteeing confidentiality of private communications. A technology which was formerly the sole preserve of the military and intelligence organisations is increasingly within reach of ordinary people.

#### *Relevance of technological issues to the review*

It is worth reflecting on the relevance of the pace of technological change for the review of the operation of the Privacy Act. In my view, one of the lessons to be learned is that it is necessary to avoid the Act being linked too closely to today's technology in case the law rapidly becomes meaningless as the technology changes. There is benefit in having the Act generally remain "technology neutral".

The challenges posed by technology are shared in other countries as well. The proliferation and adoption of new technology is just one aspect of globalisation. Accordingly, in moving to address technological challenges care should be taken to keep in step with emerging international approaches.

Nonetheless, we should not ignore the challenges imposed by technology. I have no wish for the Act to be perfectly "technology neutral" yet ineffective in protecting individual privacy when confronted with new technology. The desire for generic standards should not be allowed to hinder an effective response to known technological risks. This can sometimes be done by code of practice. Sometimes the Act should directly address a technological issue. In other cases special legislation is warranted.<sup>2</sup>

Information is now technically able to be moved and transformed with great rapidity. Technology has the ability to circumvent some traditional administrative controls. Obviously new and appropriate technical and administrative controls must continue to be applied. However, such technological challenges may mean that the *legal* controls are more important than ever. If the technology itself does not have inherent limitations as to what may be done with personal information it becomes especially important that the agency entrusted with that information constrain itself consistently with the law.

## ECONOMIC CONTEXT

There are two threads running through the international approach to the protection of privacy in the light of technological challenges. The first concerns human rights. The second, economics. The economic interest in the issues is plain from the fact that two of the main international "regulators" are the Organisation for Economic Cooperation and Development and the European Union.

#### *Origins of OECD interest*

As previously outlined, many developed countries began legislating to protect privacy during the early 1970s. During that and the preceding period there had been a greater emphasis on individual rights and legislatures responded by enacting legal protections. It

<sup>2</sup> For example I supported the creation of a warrant process for the use of telephone analysers. At recommendation 22 I propose the same for law enforcement use of covert video surveillance.

was also a period when a number of significant studies of privacy were undertaken because of a concern about technological developments.

The principal New Zealand example of 1970s privacy legislation was the Wanganui Computer Centre Act 1976. The level of interest during this period also saw two other privacy bills before the New Zealand Parliament to address privacy, the Preservation of Privacy Bill 1972 and the Privacy Commissioner Bill 1975. Sixteen years were to elapse before a resurgence of interest in privacy saw two further bills before Parliament.

A broad variety of national privacy laws was perceived as an economic problem by the OECD. In the Preface to the OECD Guidelines in 1980 it stated:

“The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one-half of OECD member countries to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

“On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

“For this reason OECD member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.”

The OECD emphasised two economic considerations which might be characterised as follows:

- *globalisation* - a recognition of the increasing interaction of countries through the transborder flow of personal data;
- *harmonisation* - the notion that consistent legislation based upon shared principles could diminish interruptions in trade while ensuring that human rights are protected.

The Council of Europe’s 1981 Convention No 108 was similarly motivated although that body was more steeped in the human rights tradition than the OECD. The OECD Guidelines and Convention No 108 provided the framework for most general data protection or information privacy laws since enacted.

#### *Globalisation and harmonisation*

The economic considerations which drove the OECD in 1980 have not diminished. Indeed they have become more profound. The transborder data flows with which the OECD group of experts were familiar in 1980 have multiplied in quantity and type. The world that we now live in, or are heading towards, is sometimes referred to as the “Information Society” - an updated version of the 1960s “global village”. The growth of the Internet, and its potential to reshape the way business and leisure are conducted, is a notable current example.

Many jurisdictions without data protection or information privacy laws, or with limited sectoral laws, have been contemplating enacting more broadly based laws because of globalisation. Typically such governments are driven by the prospects of electronic commerce. For example, the State of Victoria in Australia has announced its intention to legislate for a privacy law as part of its policy to build a network and knowledge based economy. The discussion paper released by the Minister for Information Technology and Multimedia explains that:

“The Victorian data protection regime will provide a strategic response. It will bolster business and consumer confidence in on-line transactions by committing to a minimum standard of data protection, as expressed in the Federal Privacy Commissioner’s *National Principles for the Fair Handling of Personal Information*. These principles directly address concerns about information privacy and security. Businesses will be certain that the standards they meet will be in line with national and international expectations and consumers will be able to seek redress should the standards not be met.”<sup>3</sup>

The quotation also emphasises the common wish amongst governments to legislate for privacy consistently with national and international standards. Federal countries such as Australia and Canada fear that a patchwork of laws will increase compliance costs while failing to adequately protect privacy.

#### *EU Directive on Data Protection*

Harmonisation was also one of the principal drivers of the most significant development since 1981 - the EU Directive on Data Protection of 1995. That Directive requires EU states to bring existing laws up to the minimum standard by October this year. It seeks to impose a maximum standard of privacy protection as well.

The EU Directive’s controls on transborder data flows discussed in detail later in this report,<sup>4</sup> is an economic consideration for “third countries” such as New Zealand. Indeed, this has been one of the main points of discussion since 1990 when the draft Directive was first released. From October 1998 onwards EU states will impose data export controls. European and multinational corporations which are involved in sending data to third countries for processing on an ongoing basis will have to weigh up who they can or may send personal data to.

Uncertainties as to whether a jurisdiction offers “adequate protection” bring costs for businesses yet may offer comparative advantages for jurisdictions in which adequate protection is known with certainty. In this respect the enactment of the Privacy Act in 1993 was designed to bring New Zealand agencies some comfort. Hong Kong, especially dependent upon trade, passed a similar law in 1995. A list of jurisdictions which have enacted general privacy laws, some in response to the EU Directive, since 1992 is set out at Appendix C. One can contrast the secure position of businesses in New Zealand and Hong Kong with the somewhat uncertain position of counterparts in Canada and Australia.

#### *Public sector reform*

Public sector reform has been a feature of developed countries since 1980. Reforms have been driven by various objectives including a drive for efficiency and perceived economic benefits. Privacy expectations have sometimes been a barrier to change. Typically the public sector reforms at issue have involved a function of handling of sensitive personal information being transferred to the private sector by way of outsourcing or privatisation. In some cases governments have foregone reform in particular circumstances. In other cases, governments have expressly addressed privacy concerns when making reforms.

<sup>3</sup> State Government of Victoria, *Information Privacy in Victoria: Data Protection Bill*, discussion paper, July 1998, page 8.

<sup>4</sup> See paragraph 2.8.12.

For example, Australia’s Privacy Act principally applies just to the Commonwealth public sector. Accordingly, when the present government sought to involve the private sector more closely in managing unemployment services, it needed to enact complex extensions of the Privacy Act to the relevant entities. A further bill to extend the Australian Privacy Act in response to moves to outsource a wide variety of information processing is before the Commonwealth Parliament.<sup>5</sup>

Prior to the enactment of the Privacy Act 1993 New Zealand had similar experiences. The Health Amendment Act 1988, and related amendments to the Hospitals Act and Area Health Boards Act, specifically crafted a privacy regime to take account of the privatisation of the health computer system. In the early 1990s a proposal to sell the Government Computing Service, which operated the Wanganui Computer Centre, was not seen as feasible in the absence of a general privacy law. The sale was postponed until after the enactment of the Privacy Act.

The existence of a seamless Privacy Act covering public and private sectors enables governments to take the decisions that they consider appropriate for the economy. That does not mean to say that governments ought to outsource or privatise particular functions carried out in the public sector, or ought not to do these things, merely that the Act provides privacy protection whether or not they do so. A range of choices, satisfactory from a privacy perspective, remain available to any government.

Another aspect of economic concern of government has been a wish to avoid the imposition of excessive compliance costs on businesses. The Privacy Act is a product of a desire to protect privacy adequately while, at the same time, avoiding significant administration costs for the Government or undue compliance costs on business. A significant step was taken in this regard with the study of comparative jurisdictions in *Data Privacy: An Options Paper* prepared for the Minister of Justice in 1987. That report offered clear warnings against the licensing and registration systems used in Europe and steered the Act towards a more “light handed” approach. The decision to apply the law equally to public and private sectors, and not to distinguish between automatically processed and other information, has avoided many of the complexities, demarcation problems, inconsistencies and ineffectiveness, of some overseas laws. Furthermore, the detailed study of the Privacy of Information Bill by a select committee led to a series of significant changes, many of which were directed towards minimising compliance costs.

#### *Economic considerations in the review*

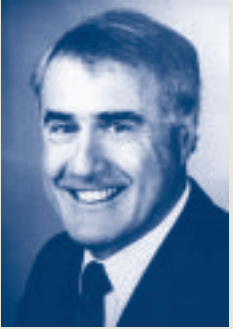
Section 14(a) directs me in to have due regard for, amongst other things, social interests that compete with privacy including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way. I have carefully taken into account a variety of the economic considerations as I have undertaken this review. In particular, I have sought to:

- be alive to those features of the Act which were intended by the Government, or the Select Committee, to ensure that the Act operated in an efficient and satisfactory way and to review and if necessary enhance those features;
- consider ideas for minimising compliance or administration costs while effectively protecting privacy;
- examine the emerging international approach to transborder data flows and to consider whether any change to our Act is warranted;
- ensure that the Act provides “adequate protection” in terms of the standards in the EU Directive on Data Protection.

## LEGISLATIVE HISTORY

### *Introduction*

While there are many features in the Privacy Act without precedent in New Zealand legislation, the Act also represents a consolidation and evolution of a number of earlier



**Rt Hon Geoffrey Palmer:**  
Commissioned the 1987  
*Data Privacy: Options  
Paper* which shaped  
subsequent information  
privacy initiatives.

PHOTO: ALLAN JENKINS



**Tim McBride:** Author of  
the 1984 *Privacy Review*  
and 1987 *Data Privacy:  
Options Paper*.

PHOTO: OFFICE OF THE  
PRIVACY COMMISSIONER.

<sup>5</sup> Privacy Amendment Bill 1998 (Australia).

legislative initiatives. The Act also contributes to implementing New Zealand’s international obligations.

Features of the Privacy Act which represent a continuation of the existing New Zealand statutory tradition include:

- vesting in the Privacy Commissioner functions formerly carried out by the Wanganui Privacy Commissioner, Human Rights Commission, Ombudsmen and Information Authority;
- continuing access rights formerly contained in the Wanganui Computer Centre Act 1976, Official Information Act 1982 and Local Government Official Information Act 1987;
- consolidating aspects of the Wanganui Computer Centre Act 1976, Health Amendment Act 1988 and related health sector legislation, and the Privacy Commissioner Act 1991.

The legislation directly implements the OECD Guidelines which New Zealand accepted in 1980. It also represents a measure to protect people from arbitrary interference with their privacy and to provide a remedy for any such interference. New Zealand assumed such obligations when it signed the International Covenant on Civil and Political Rights in 1968 and later ratified it in 1978.

In the following material I outline some of the influences which have helped to shape our legislation. I mention some of the previous bills, statutes, official reports and processes of relevance. The material should be read together with Appendix D which lists many of the key influences since 1972 and Appendix H, which lists provisions in earlier statutes upon which the Act is based.

It should be plain from the material that the Act is not a “bolt from the blue”. It is the outcome of many years of study of the issues informed by forays into legislation covering particular computer databases and sectors and governing access to information. The Act’s complaints resolution processes draw upon well tested and successful models pioneered in New Zealand since 1962 in the Ombudsman Act and adapted in 1977 and 1982 for discrimination complaints and information access reviews.

#### *The 1970s - Experimental national legislation*

Many countries began legislating to protect privacy from the early 1970s as a response to concerns about the effects of modern technology on individuals. The first privacy bill brought before the New Zealand Parliament was the Preservation of Privacy Bill introduced in 1972 by Squadron Leader Drayton MP. Mr Drayton’s bill ran to just 22 clauses. It would have established a Privacy Commissioner to be the registrar of all computer installations in New Zealand. The owners of computer installations would have been obliged to supply a copy of any information programmed into the computer system to the individual concerned within three months. Thereafter the individual could obtain a printout on request.

As is common with private members’ initiatives the Preservation of Privacy Bill was defeated on its introduction. However, some points of interest may be noted:

- the Parliamentary debate shows bipartisan concern about privacy and the challenges posed by computer databanks - which foreshadows the fact that both a new Labour, and a subsequent National, government were to propose legislation within four years;
- this was the only New Zealand bill ever to propose registration of computer systems - registration has never found favour here notwithstanding its adoption in the UK and throughout Europe;
- this bill initiated the use of “privacy” in preference to the European term “data protection” and was the first to propose a “Privacy Commissioner” - features found in every subsequent bill.

The first Government privacy bills also appeared in the earlier 1970s. The Private Investigators and Security Guards Act 1974 might be counted as the first tentative step since



**Squadron Leader Drayton MP:** Introduced the first privacy bill to the New Zealand Parliament in 1972.

PHOTO: ALLAN JENKINS



**Hon Dr Martyn Finlay:** Minister of Justice responsible for the introduction of New Zealand’s first Government bill to establish a Privacy Commissioner. The Privacy Commissioner Bill 1975 did not survive the subsequent change of Government.

PHOTO: ALLAN JENKINS



**Hon Arthur Faulkner:** Minister of State Services responsible for introducing the Wanganui Computer Centre Bill in 1975. This pioneering law was notable for being both New Zealand's first data protection law and its first freedom of information law.

PHOTO: ALLAN JENKINS



**Hon David Thomson:** As Minister of Justice oversaw the creation of the Human Rights Commission which had, amongst its other responsibilities, an inquiry function in respect of privacy.

PHOTO: ALLAN JENKINS



**Hon Peter Gordon:** As the new National Minister of State Services, John Gordon was responsible for the enactment of the Wanganui Computer Centre Act 1976, introduced by the previous government.

PHOTO: ALLAN JENKINS

its long title made it clear that it was intended to afford “greater protection to the individual’s right to privacy against possible invasion by private investigators”. However, two bills introduced in 1975 fall more clearly into the mainstream of information privacy initiatives. These were the Privacy Commissioner Bill, introduced by Hon Dr A M Finlay, Minister of Justice, and the Wanganui Computer Centre Bill, introduced by Hon A J Faulkner, Minister of State Services.

The Privacy Commissioner Bill would have established a Privacy Commissioner with an inquiry and reporting function but without a complaints jurisdiction. In this respect, it has much in common with the bill which bore the same name in 1991. In the words of Dr Finlay:

“The Commissioner will act as a sounding board and gather information in the field of privacy with the ultimate object of assisting Government departments decide what, if anything, needs to be done in the way of legislation or otherwise.”

It was also anticipated that further functions would be conferred upon the Privacy Commissioner by other legislation including, in the first instance, under the Wanganui Computer Centre Bill.

The Privacy Commissioner Bill did not survive a change of government in 1975. The new National Government instead conferred a limited privacy jurisdiction, again excluding complaints, upon the Human Rights Commission established in 1977. However, the Wanganui Computer Centre Act 1976 was enacted into law. Amongst other notable features that Act established:

- New Zealand’s first Privacy Commissioner;
- New Zealand’s first freedom of information law with the Commissioner operating a bureau enabling individuals to have access to information held about them on the computer;
- institutional and legal controls to protect privacy in the face of the large new computer databank.

During the 16 years of the 1976 Act’s operation four persons were to hold the post of Privacy Commissioner (see Appendix D). Sir George Laking was the first Commissioner. He relinquished the post as the administrative load became too much given his combined role as Ombudsman. Amongst other things, Sir George established systems to enable individuals to obtain access to their criminal history information. Mr R A (later Justice) McGechan, then Deputy Chairman of the Wanganui Computer Centre Policy Committee, temporarily served as Commissioner until Sir James Wicks commenced a five year term in 1978. During his period as Commissioner, but separate from those tasks, Sir James was to chair the Committee of Inquiry into the Administration of the Electoral Act following registration difficulties associated with the 1981 election. Paul Molineaux was to serve two five-year terms as Wanganui Commissioner starting in 1983. In the event, Mr Molineaux was to be the last such Commissioner appointed under the 1976 Act sharing the last year of his appointment as Wanganui Computer Centre Privacy Commissioner with my first year as Privacy Commissioner under the Privacy Commissioner Act 1991.

#### *The 1980s - International standard setting, local study and sectoral legislation*

The 1976 Act was hailed as a world class data protection and freedom of information measure. However, on both counts the law soon became outclassed. A far more sophisticated approach to data protection was expected following the OECD Guidelines (1980) and Convention No 108 (1981) while much more extensive freedom of information legislation was enacted in New Zealand in 1982. The Wanganui Computer Centre Privacy Commissioner endorsed calls for new, more comprehensive, privacy legislation describing the existing law in his 1989 annual report as “piecemeal, fragmented and incomplete”.

In addition to the OECD and Council of Europe standard setting at international level, there were a variety of privacy studies undertaken in the 1980s. For example, in New Zealand the 1984 *Privacy Review*, prepared pursuant to the Human Rights Commission Act 1977, provided a resource for the promotion of debate about privacy.

Across the Tasman, the Australian Law Reform Commission published its two volume *Privacy* report. The 1983 report was one of the most comprehensive ever on the subject of information privacy. The Australian Commission was headed by Justice Michael Kirby, who had earlier chaired the OECD Group of Experts which drafted the OECD Guidelines, and had amongst its researchers Kevin O'Connor, later to become Australia's first Privacy Commissioner. The Commission proposed a draft privacy bill, parts of which formed the basis of the Australian Privacy Act 1988. The Australian Act was a model from which the New Zealand Act was to heavily borrow.

The access and correction provisions in the Act were to be derived in large measure from the Official Information Act 1982, which was itself based upon recommendations of the Committee on Official Information (“the Danks Committee”). A similar committee, chaired by Sir Alan Danks, was constituted as the “Information Authority” pursuant to the 1982 Act. The Information Authority functioned for five years before going out of existence.

In 1985 the Information Authority released a discussion paper concerning personal information and the Official Information Act. In 1987 it followed with a further discussion paper putting forward recommendations for reform to address information privacy concerns. The paper suggested principles to govern the collection and use of personal information and proposed clauses which could be included in the Official Information Act. The process finally led to a 1988 report to Parliament on the subject of the collection and use of personal information.<sup>6</sup> The report was not implemented in the fashion recommended but was undoubtedly an influence upon the later drafting of the Privacy of Information Bill.

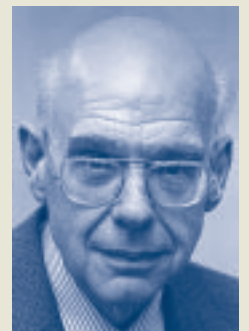
The Information Authority report was released at the time of the privatisation of the health computer system. As a result, amendments were made to the Health Act, Hospitals Act and Area Health Boards Act, to craft a privacy regime governing the collection, holding, use and disclosure of personal information consistent with aspects of the Information Authority's report. In addition to the more usual security obligations, access and disclosure constraints, the amendments might be considered the first provisions in New Zealand's law implementing the OECD collection limitation principle. The 1988 health sector privacy legislation was repealed in 1993.

The Broadcasting Act 1976 was a further piece of specific sector privacy legislation. That Act required programme standards to be consistent with the privacy of the individual and enabled complaints to be taken to the Broadcasting Tribunal. This was carried forward into the Broadcasting Act 1989 which also provided for compensation for privacy complaints, unlike other breaches of standards. The existence of that provision is relevant to the debate over the significance of the exemption from the Privacy Act of the news media in their news activities. Unlike the print media, there are privacy standards applicable to the broadcast media under which complaints may be brought and compensation obtained.

#### *The 1990s - Comprehensive privacy legislation*

Prior to the 1990 election officials had already undertaken preparatory work to draft information privacy legislation. This work followed through on the 1987 *Data Privacy: An Options Paper* and the 1988 Information Authority report. It may also have been in contemplation of government data matching.

<sup>6</sup> Information Authority, *Report of the Information Authority on the Subject of Collection and Use of Personal Information*, May 1988.



**Sir Alan Danks:** Chaired the Committee on Official Information which recommended the repeal of the Official Secrets Act 1951 and the enactment of the Official Information Act. Sir Alan went on to chair the Information Authority which recommended enactment of a law governing collection and use of personal information.

PHOTO: NORTHERN ADVOCATE



**Hon Jim McLay:** Minister of Justice responsible for the enactment of the Official Information Act 1982 in the final term of the Muldoon government.

PHOTO: ALLAN JENKINS

By the time of the 1990 election both major parties were committed to information privacy legislation. The change in government led to a delay in the public production of a bill. As a spur to action, the opposition Labour Party introduced its own bill in the name of Peter Dunne MP. Peter Dunne's Information Privacy Bill 1991 was followed in the same year by the new National Government's Privacy of Information Bill. The two bills were very similar except the Dunne Bill proposed to continue the function of the Wanganui Computer Centre Privacy Commissioner to act as a bureau for releasing information to individuals from the Wanganui Computer Centre.

Both bills were referred to the Justice and Law Reform Select Committee. The bills stirred a degree of controversy and attracted quite a number of submissions. Only the Government bill progressed.

One of the prime objectives of the Government bill was to authorise and regulate a government data matching which was referred to as "information matching" based upon a similar Australian law passed the previous year.<sup>7</sup> The tackling of welfare fraud was a plank in the Government's 1991 social welfare reforms and so it did not wish to see significant delay in the introduction of information matching. However, it was plain that the privacy bills would require a great deal of study and consultation. The Government took the decision to split off from the Privacy of Information Bill those parts establishing a Privacy Commissioner and governing information matching and enact them separately from the rest of the bill.

Accordingly, the Privacy Commissioner Act 1991 was enacted in December 1991 just four months after the Privacy of Information Bill had been introduced without the Select Committee having studied the balance of the bill. This was a controversial move. The Opposition voted against the 1991 Act.

The Select Committee studied the proposals for information matching and made significant changes to the bill. In particular, information matching programmes were no longer to be authorised by the Privacy Commissioner but instead by legislation. The Commissioner was to have a reporting and oversight role but not, at this stage, a complaints function. Concern was expressed as to how effective such a Commissioner could be. The Government's position was that this was a temporary arrangement pending Parliamentary consideration of the balance of the Privacy of Information Bill.

The Select Committee continued its study of the Privacy of Information Bill during 1992 and early 1993. Having heard submissions, a great deal of change was proposed. In conducting this work the Committee was to have my assistance as the first Privacy Commissioner appointed under the 1991 Act. I used the opportunity to familiarise myself with privacy issues and to meet with many of the organisations which had expressed concerns about the bill in their submissions. The Committee acknowledged it was greatly assisted by Margaret Nixon of the Department of Justice and by Geoff Lawn of the Parliamentary Counsel Office.

Amongst notable changes made to the bill, the Select Committee:

- provided for codes of practice to be issued by the Privacy Commissioner;
- introduced an exemption for the news media and members of Parliament;
- created special controls on public register personal information;
- dropped some of the information privacy principles from the bill but created a new one concerning unique identifiers;
- permitted private sector agencies to charge for access.

The Select Committee's work was accelerated as it became apparent that it would be desirable for the Privacy Act, as the bill was now to be known, to be in place in time for the public sector health reforms due to begin in the middle of 1993. It was recognised that there would be public concerns about the protection of sensitive health information as a result of those reforms.



**Peter Dunne MP:**  
Introduced the Information Privacy Bill 1991. This Opposition initiative spurred further interest in the issue and set the scene for eventual bipartisan support for the enactment of the Privacy Act.

PHOTO: P DUNNE



**Rt Hon Douglas Graham:**  
Minister of Justice responsible for the introduction of the Privacy of Information Bill. While the bill was initially controversial, the Minister guided the Privacy Act 1993 to eventual enactment with unanimous Parliamentary support.

PHOTO: WOOLF LTD

<sup>7</sup> Data-matching Program (Assistance and Tax) Act 1990 (Australia).

*Some reflections on legislative history*

The bill was passed through Parliament on 5 May 1993 and received Royal Assent 12 days later. The Privacy Act consolidated the limited 1991 legislation and produced a privacy law more comprehensive than any outside Europe. The Select Committee had done such a careful job of addressing concerns that had been raised in submissions on the bill and in Parliament during the enactment of the Privacy Commissioner Act 1991 that it was finally passed with complete bipartisan support.

In undertaking the review of the Privacy Act I have been conscious of what has gone before. My overall view of the Act is that it is well conceived and approaches the task in an appropriate manner. Naturally, there is room for improvement. Indeed, I have made over 150 recommendations. However, a study of our legislative history, and that of other similar jurisdictions, suggests to me that the Act is indeed firmly on the right track.

0

25



**Hamish Hancock MP:**  
Responsible, as Chair of  
the Subcommittee of the  
Justice and Law Reform  
Select Committee, for  
studying the Privacy of  
Information Bill and  
recommending changes  
to the renamed Privacy  
Act 1993.

PHOTO: H HANCOCK

