Fourth supplement to first periodic review of the operation of the Privacy Act 1993

Report by the Privacy Commissioner to the Minister of Justice supplementing *Necessary and Desirable: Privacy Act 1993 Review* (December 1998) and the First, Second and Third Supplements to that report

---

15 May 2008

Privacy Commissioner
Te Mana Matapono Matatapu

KEY HIGHLIGHTS

This supplementary report draws attention to selected developments in the privacy landscape over the last 4 years. Outside New Zealand these have included, for instance:

- active international privacy standard setting: the APEC Privacy Framework (2005), the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy (2007) and the APEC Privacy Pathfinder (2007+)
- a major review of Australian privacy law
- greater awareness of privacy risks in security breaches and identity fraud
- innovation in regulatory responses to privacy challenges such as breach notification, cross-border enforcement cooperation, national telemarketing opt out databases.

Domestically some notable developments are referred to such as:

- significant new information statutes like the Evidence Act 2006, Unsolicited Electronic Communications Act 2007 and the proposed Criminal Disclosure Act
- court cases clarifying aspects of privacy law by confirming the meaning of 'tribunal' and the ability to declare tribunal applicants as vexatious litigants.

A significant proportion of the report brings relevant developments to the attention of anyone concerned with earlier recommendations. In addition the report also provides several new recommendations.

These include recommendations:

- to require mandatory security breach notification
- to empower the Commissioner to conduct audits
- to explore establishing a national do-not-call database as a response to telemarketing and to consider regulating automatic dialling machines
- to study the APEC 'accountability principle' as a response to the risks of trans-border data flows
- for officials to consider whether any amendments are needed to cope with catastrophic natural disasters.

FOURTH SUPPLEMENT TO FIRST PERIODIC REVIEW OF THE OPERATION OF THE PRIVACY ACT 1993

Contents

FOURTH SUPPLEMENT TO FIRST PERIODIC REVIEW OF THE OPERATION OF THE PRIVACY ACT

1. INTRODUCTION

1.1 The Privacy Commissioner is required periodically to review the Privacy Act's operation and report any recommendations for necessary or desirable amendments.[1] My predecessor, Bruce Slane, commenced a major review in 1997 and submitted his report *Necessary & Desirable: Privacy Act Review 1993* in November 1998. He updated that report with two supplementary reports in April 2000 and January 2003 and I provided a further supplement in December 2003. This supplement further updates those earlier reports in response to developments over the last four years.

1.2 In December 2003 when I last submitted an update, I had understood from officals that an amendment bill was imminent. I am concerned that another four years has since elapsed. It now seems unlikely that 2008 will be the year in which a significant portion of the accepted recommendations will see the light of day in an amendment bill to Parliament. However, I hope that the trans-border data flow issues can be dealt with as a matter of urgency; and that following the Law Commission's report on its privacy reference, necessary amendments to the Act can be made.

1.3 The update refers to developments, such as relevant law changes or international instruments, bearing upon existing recommendations. I offer a small number of additional recommendations arising from developments since January 2004. I hope that this further update will be useful to officials, to any select committee called to study implementing legislation and to members the public having an interest in the original *Necessary & Desirable* report or making a submission. It will also be a resource for the Law Commission in its current review of privacy.

1.4 As with the earlier updates, the recommendations are ordered and numbered in such a way that they fit with the original recommendations. For convenience, a consolidated set of recommendations from the 1998 report and four supplements is available as a separate document.

1.5 Section 26 requires me to review the operation of the Act periodically. The substantial delay in official evaluation of the recommendations from the first review, and the implementation of any recommendations adopted, has caused difficulty in terms of my statutory responsibilities to commence a second review. Thus far, I have concluded that it is 'not practicable' - in the words of section 26 - to actively embark upon a further review until there is clarity as to the adoption or rejection of earlier recommendations. I am looking forward to seeing implementing legislation since so much has happened since 1998 warranting a more careful examination than is possible in these updates.

Marie Shroff
Privacy Commissioner
15 May 2008

---

[1] Privacy Act 1993, section 26.

2. FURTHER NECESSARY OR DESIRABLE AMENDMENTS AND UPDATE ON EARLIER RECOMMENDATIONS

2.1 Recommendation 9: Meaning of "tribunal" confirmed by High Court

The Privacy Act defines 'tribunal' and uses that term as part of an exception to the meaning of 'agency' (fundamental to the scope of application of the information privacy principles) and within an exception to several information privacy principles. *Necessary & Desirable* noted that a private organisation had described one of its internal decision or recommendatory organs as a 'tribunal' and had tried to claim the benefit of exceptions to the Act. It was recommended that consideration be given to making the statutory definition more explicit to show that tribunals are limited to statutory tribunals forming part of the New Zealand administrative or judicial structure.

Unfortunately, the issue has continued to arise since 1998 in relation to the same organisation. However, the legal question has recently been settled in the High Court on a case stated.[2] The High Court was asked the question:

> "Whether the word 'tribunal' in section 2(1)(b)(viii) of the Privacy Act 1993 is capable of applying to a non-statutory tribunal and if so, what criteria (if any) must such a non-statutory tribunal satisfy (apart from the exercise of judicial functions) so as to qualify as a 'tribunal' under that provision?"

Justice Cooper delivered his judgment on 19 February 2008 and ruled that the word 'tribunal' used in the definition of 'agency' is not capable of applying to a non-statutory tribunal.[3]

The High Court judgment confirms the position that the Privacy Commissioner has consistently held. Recommendation 9 would have made that position plainer, for anyone in doubt, without the need to resort to litigation. Given the judgment, there is probably no longer any need to amend the definition as early recommended.

I therefore withdraw recommendation 9.

2.2 Recommendation 11: New definition of "document" in Evidence Act 2006

In *Necessary & Desirable* it was noted that the definition of 'document' used in the Privacy Act had been the result of earlier careful drafting with a lineage stretching back to a 1980 amendment to the Evidence Act 1908. It was noted that the Evidence Act was under review and likely to result in more modern definition. A new Evidence Act was enacted in 2006. The new definition provides:

> **"document** means -
> (a) any material, whether or not it is signed or otherwise authenticated, that bears symbols (including words and figures), images, or sounds or from which symbols, images, or sounds can be derived, and includes-
> (i) a label, marking, or other writing which identifies or describes

[2] The Director of Human Rights Proceedings v. The Catholic Church for New Zealand
[3] The Director of Human Rights Proceedings v. The Catholic Church for New Zealand HC AK CIV 2006-404-006162 [19 February 2008], Cooper J, paragraph 73.

a thing of which it forms part, or to which it is attached:
(ii) a book, map, plan, graph or drawing:
(iii) a photograph, film, or negative; and
(b) information electronically recorded or stored, and information derived from that information".[4]

As earlier recommended, consideration should be given to aligning with the new definition of "document" in the Evidence Act.

2.3 Recommendation 17A: Australian developments with "anonymity principle"

The first supplementary report drew attention to the "anonymity principle" contained in the Australian National Privacy Principles (NPPs). The NPPs were to be incorporated into state and federal law in Australia and it was recommended that something similar be considered for New Zealand.

The concepts of anonymity and pseudonymity have become important in privacy discourse since in this electronic age there is a need to challenge the practice of amassing ever more personal information. Simply protecting the data held is not enough, Some technologists have tried to rise to the challenge of preserving privacy by developing Privacy Enhancing Technologies or "PETs" based upon the ability to transact electronically without revealing one's identify. Australia has been something of a leader internationally in enshrining an anonymity principle as a core element of its privacy law although a number of other countries including New Zealand have incorporated the principle in specific contexts, such as telecommunications[5] or road tolling.[6]

In its review of the Australian Privacy Act, the Australian Law Reform Commission reviewed the anonymity principle.[7] The ALRC endorsed the continuation of the principle, recommended that its application be expanded from the private sector to also include the public sector (in a new unified privacy principle - UPP) and proposed that the principle recognise the key concept of pseudonymity. While anonymity requires that no personal information about an identifiable individual be processed, pseudonymity anticipates the individual transacting using a pseudonym that bears no relation to the individual's usual name.

The proposed new unified privacy principle would read as follows:

> **"UPP1 Anonymity and pseudonymity**
> Wherever it is lawful and practicable, individuals, when transacting with an agency or organisation should have the clear option of either:
> (a) not identifying themselves; or
> (b) identifying themselves with a pseudonym provided this would not be misleading."

---

[4] Evidence Act 2006, section 4(1).
[5] See, for example, Germany's Telecommunications Data Protection Act of 1997.
[6] See, for example, New Zealand's Land Transport Management Act 2003, section 51, which provides that toll operators must offer alternative methods of payment and that "at least one of the methods of payment must be a method that does not record personal information in relation to the person paying the toll."
[7] Australian Law Reform Commission, *Review of Australian Privacy Law: Discussion Paper 72*, September 2007, volume 2, chapter 17. Note that the ALRC proposal may differ in its final report.

When recommendation 17A is further considered, the new Australian principle should be borne in mind and preferred over the earlier wording.

2.4 Recommendation 22: Law Commission surveillance powers project

It was recommended in *Necessary & Desirable* that consideration be given to establishing a judicial warrant process in relation to covert video surveillance in the investigation of offences. It is encouraging to note that this issue has been the subject of thorough study by the Law Commission. A series of recommendations is made in the Law Commission's Report 97, *Search & Surveillance Powers*, June 2007.

I note that recommendation 22 may be given effect to in the implementation of the Law Commissions surveillance powers project.

2.5 Recommendation 23A: Privacy breach notification

Information privacy principle 5 requires agencies to take reasonable security safeguards in relation to the information they hold. Of course, security breaches sometimes happen as risk is never entirely eliminated. In the last four years there has been increasing interest overseas on the subject of security breaches and regulatory attention has been focused upon the usefulness of breach notification to affected individuals.

A number of large security breaches led lawmakers, initially at state level in the US, to require affected individuals to be notified when record had been released through a security breach. The first such law, in California, came into effect in 2003. Since that time about 35 states have followed suit and enacted broadly similar laws. Particularly as a result of these and similar laws, there are now almost daily stories of major security breaches affecting the records of thousands and sometimes millions of individuals.

A security breach affecting the records of a single person may have a significant privacy impact for that person. In addition the issue has been associated with identity fraud. The fear is that in addition to any other privacy risks, criminals may be targeting or obtaining records that have been left unprotected and that this may adversely affect individuals by, for example, enabling criminals to appropriate individuals' identities in order to obtain credit or otherwise defraud the affected individuals or institutions.

Requiring individuals to be notified of a relevant breach is an attempt to empower them to take necessary and timely steps to protect themselves or otherwise recover their position. Although the attention to breach notification, and the enforcement of it through privacy laws, is a relatively new phenomenon the concept itself is consistent with usual data protection principles such as the OECD's Security Safeguards, Openness, Individual Participation and Accountability Principle.

In 2006 my office commenced a project to study the benefits of breach notification. An opportunity arose during a staff secondment to participate in policy development work on the Privacy Commissioner of Canada's privacy breach guidelines. I was convinced of the usefulness of encouraging New Zealand agencies to notify individuals of breaches affecting them where there was good reason to do so (particularly where the individual needed that knowledge to take some step to protect themselves that the agency could not itself take). During Privacy Awareness Week in August 2007 I released a proposed set of

privacy breach guidelines, based on the Canadian precedent, to gauge the views of New Zealand business and others as to the appropriateness here. Considerable support was received and I finalised and released their privacy breach guidelines early in 2008.[8] As with the Canadian guidelines, these are voluntary. However, I do believe that there is a good case for legislation requiring government agencies and private sector businesses to notify customers where a security breach puts those customers at risk.[9]

I recommend that New Zealand law should provide for mandatory security breach notification. This report is not the place to go into full detail but I believe that the Law Commission will be well placed to include a study of this topic in its current privacy reference. We are fortunate the subject has been given recent careful attention by the Australian Law Reform Commission which has recommended breach notification requirements for that country.[10]

Based on my office's work to date, I will briefly highlight three aspects that I suggest should influence the approach to be taken:

- risk assessment
- international compatibility
- emphasising agency responsibility

Risk Assessment

In my view, risk assessment needs to feature in the approach taken (whether or not the phrase actually appears in the law). In essence, the notification should be mandatory where the risks to the individual warrant the notification and where that notification will serve a useful purpose. There are some breaches that do not warrant notification. A requirement to 'over-notify' where the risks do not warrant it can be counter productive and fall short of best practice regulation.

International Compatibility

The voluntary guidelines that I released were closely modelled upon Canadian guidelines. Adopting the guidelines in New Zealand was a small but noteworthy step in seeking to promote coordinated privacy guidance and regulation. I am aware that at least one Australian jurisdiction is also planning to adopt guidelines based on the New Zealand guidelines.[11] One of the challenges for addressing privacy issues in this global electronic economy is the attempt to align national requirements. Consideration should at least be given to the merits of maintaining alignment with the approach in Canada or that recommended in Australia. There may be benefits to businesses, and indirectly to consumers, if businesses operating across jurisdictions can seamlessly comply with such a new requirement.

---

[8] Privacy Commissioner, Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist, February 2008.

[9] See Privacy Commissioner media release 'Good Case for Mandatory Breach Notification Law', 21 February 2008.

[10] Australian Law Reform Commission Discussion Paper 72, *Review of Australian Privacy Law*, September 2007, chapter 47.

[11] Office of the Victorian Privacy Commissioner, 'Avoiding Catastrophes', 6/4 *Privacy Aware*, Summer 2007/08.

Emphasising agency responsibility

In my view, the mandatory requirement should be for the agency to notify the affected individuals rather than principally to notify my office.[12] Some overseas jurisdictions have proposed models of notification that would require agencies simply to notify the regulator which would then order whether or not a notification is required. In my view this runs counter to the ethos of the information privacy principles that places obligations with agencies and then expects them to discharge those obligations. Breach notification is not necessarily a more serious responsibility than many of the others they currently possess. While this is a matter to be further studied, there might be a useful role for the regulator to order disclosure in exceptional circumstances, for example where the agency is unwilling to act or is too slow in doing so.

> ***Recommendation 23A***
> *The Privacy Act should include an obligation requiring agencies to notify affected individuals where a security breach by the agency puts the individual at risk.*

2.6 Recommendations 25 & 25B: Direct marketing regulatory initiatives

Direct marketing through secondary use of information obtained for other purposes is a perennial privacy issue in most jurisdictions. It is difficult in the context of mass marketing to use individualised dispute resolution or compliance mechanisms like complaints investigation or litigation that focus in detail (and at some cost) upon each case. Instead clearer 'black and white' rules for direct marketing are often desired as a supplement to general privacy principles.

Since 1998 there have been developments that reinforce the recommendation that the Privacy Act would be improved by supplementary rights targeted at facilitating opting out of direct marketing.

Europe, like New Zealand, has generic privacy laws that provide a general level of principles that seek to deal with all information privacy issues. These laws are generally based upon the EU Data Protection Directive of 1995.[13] As noted in *Necessary & Desirable* the EU Directive gave individuals an explicit right to object to direct marketing. That right influenced the 1998 recommendation.

The rights of European citizens have now been supplemented by the EU Directive on Privacy and Electronic Communications of 2002.[14] This provides explicit rights, for example, prohibiting the use of automated calling machines, fax or electronic mail for the purposes of direct marketing unless subscribers have given their prior consent. This obviously goes further than a mere right to opt out.

Unsolicited direct marketing by means of electronic mail has been a worldwide problem not merely because of privacy concerns but also because of the nuisance value and

---

[12] Of course my office (and other relevant regulators) should be copied into notifications and my office is available as a resource that can be consulted by agencies in considering their responsibilities and options in the event of a breach. .

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

fraudulent behaviour. Generic data protection and privacy laws have been unable on their own to provide a solution.

An international response has been to promote a consistent and coordinated approach to spam. One key initiative has been the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws against Spam. Consistent with the international approach, and modelled upon earlier Australian law, New Zealand enacted the Unsolicited Electronics Messages Act 2007.

Telemarketing is another area in which there have been developments. In 2003 the US "National Do Not Call Registry" began operation. This allows consumers to opt out of receiving telemarketing calls at their home or on their cell phones. Over 145 million registrations had been received by 30 September 2007. Both Australia[15] and Canada[16] have now moved to establish national 'do not call' registers for individuals to opt out of telemarketing in 2006 and 2007. Hong Kong is also implementing statutory do-not-call registers for telephone, fax and SMS. [17]

New Zealand has been spared the worst excesses of telemarketing that have plagued Americans at their dinner tables for generations. However, it does seem evident that there is more telemarketing than there used to be. Some of this comes from overseas. One factor that has inhibited cross-border telemarketing into New Zealand had been the physical distance from other countries. However, the substantial lowering of long-distance call rates together with the greater quality and take up of VOIP means that particular protection is rapidly disappearing.

Accordingly, while the Unsolicited Electronic Messages Act will address part of the issue anticipated by Recommendation 25, there remains unfinished business. In particular consideration should be given to:

- the regulation of automated calling machines – an irritant to many people that the Privacy Act alone cannot solve as personal information is only sometimes involved in operating those machines
- unsolicited telemarketing – which many people find objectionable.

> ***Recommendation 25B***
> *Consideration should be given to the merits of a national system, established under statute, to control the use of automated dialling machines and enable individuals to opt-out of telemarketing.*

2.7 Recommendation 28A: Unique identifier controls

Principle 12 has a somewhat different 'feel' to the other principles given that it has four parts, each having slightly different objectives, and a more prescriptive approach than other principles. Furthermore, the prohibition in principle 12(2), has just one exception unlike the multiple exceptions to several of the other information privacy principles.

---

[15] Telecommunications (Do Not Call Register) Act 2006. See also the Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007.
[16] Canada Radio-telephone and Telecommunications Commission, Telecom Decision CRTC 2007-08, Unsolicited Telecommunications Rules Framework and the National Do Not Call List, 3 July 2007.
[17] Unsolicited Electronic Messages Ordinance 2007.

Australian developments

Principle 12 is also unusual in being an original New Zealand creation whereas principles 1 – 11 are modelled on information privacy principles in the Australian Privacy Act. The information privacy principles in the Australian Act applied only to public sector agencies whereas, of course, the New Zealand principles apply equally to public and private sector agencies. However, when Australia devised a set of privacy principles suitable for the private sector – to become known as the National Privacy Principles (NPPs) - they included an identifier principle not found in the Australian information privacy principles. NPP7 was modelled upon New Zealand's information privacy principle 12.

It is therefore noteworthy that the Australian Law Reform Commission has recently completed a review of NPP7. It has recommended the principle's continuation into a new "Unified Privacy Principle 10" (UPP10) to cover both the public and private sectors in Australia.[18]

In one point of difference the existing Australian NPP7, and the proposed replacement UPP10, include various exceptions to the prohibition to re-assignment.[19] These are some of the exceptions also found in the other Australian and New Zealand privacy principles. The absence of a range of exceptions to information privacy principle 12(2) was not identified as an operational problem at the time of the 1998 review. However, some issues have become more apparent in the ensuing years. Indeed there has been a need to issue a series of codes of practice to provide exemptions from principle 12(2).[20] Issues have also arisen with respect to the use of departmental unique identifiers to combine governmental administrative data to create longitudinal datasets for statistical use. The Australian experience of an identifier principle containing a range of exceptions should be considered the next time principle 12 is reviewed.

Identity theft

The importance of careful controls on unique identifiers have become more apparent due to a greater appreciation of the risks of identity theft. North American experience has suggested that easy availability of unique identifier information can be problematic with respect to identity fraud. Better security practice is an appropriate response. North American research has also shown how data sets which have had the obvious personal identifiers removed (such as name and address) may still be vulnerable to re-identification and the attendant privacy risks, where unique identifiers or more general identifiers remain with the data (such as postal codes).[21]

The US has a national identifier known as the Social Security Number (SSN). It has long been known that poor privacy and security practice in relation to the SSN was creating problems. However, in recent years those problems have been hugely magnified through developments such as the availability of SSNs on the Internet and an apparent rise in criminal activity to obtain personal data. As a result, the US is paying more attention to

---

[18] See Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law*, September 2007, Chapter 27. Note that the ALRC's proposal may change when finalised.

[19] See UPP10.3 and 10.4.

[20] For example, codes have provided exemptions in relation to unique identifiers for health practitioners, patients, members of superannuation schemes, students and people being processed through the justice system.

[21] See, for example, the research of Associate Professor of Computer Science, Technology and Policy, Latanya Sweeney, Carnegie Mellon University. Considerable work in the area of re-identification risk has also been undertaken in Canada by Dr Khaled El Eman, Associate Professor at the University of Ottawa.

enforcement of existing controls on the SSN and introducing new controls. For example, in response to public fears of identify theft a growing number of states have enacted statutory restrictions on the use of SSNs. As at the beginning of this year, 29 states had laws affecting the handling of SSNs which typically include prohibitions on:

- publicly displaying, intentionally communicating or otherwise making an SSN available to the general public
- intentionally printing a SSN on any card required to access goods or services
- requiring an individual to transmit his or her SSN over the internet, unless the connection is secure or the SSN is encrypted
- requiring an individual to use their SSN to access a website, unless a password, unique pin or other authentication is also required
- printing a SSN on any materials that are mailed to the individual, unless required by law.[22]

One requirement missing from principle 12, but present in some of the American laws, is controls upon the public display of SSNs. If the unique identifier is printed on common documentation, this can fall into the hands of people that should not have that number. In the US, obtaining an individual's SSN maybe the key to accessing other holdings of information about that person.

A related response to the same security concerns has been a worldwide move to encourage number truncation in relation to credit card receipts and similar documents. The best example of this is the Payment Card Industry (PCI) Data Security Standard which requires participants in that standard to mask primary account number data when displayed.[23] What this means is that a credit card receipt given to the customer may show, as a maximum, the first six and last four digits. This security initiative does not inhibit the merchant's proper processing of credit cards or other payments since the full data can be displayed on their copy of the transaction documentation.

Hong Kong has also tightened up its requirements on the display of their identification number.[24]

The usefulness of controls on the display of unique identifiers on documentation is not limited to credit card numbers or the SSN. For example, one study found it possible to find out information about individuals from discarded boarding passes.[25]

Recommendation 28A

The Law Commission or officials, in further reviewing principle 12, should usefully have regard to:

(a) the Australian experience and proposals with its identifier principle

(b) the usefulness of including exceptions to principle 12(2)

(c) the merit of including controls in principle 12 to encourage number truncation or other ways of controlling the public display of unique identifiers.

---

[22] A summary of developments in the US can be found in Sidley Austin LLP, Information Law & Privacy Update: New Laws Significantly Restrict Handling of Social Security Numbers, 23 January 2008.

[23] Security Standards Council, Payment Card Industry (PCI) Data Security Standard, versions 1.1, September 2006, Clause 3.3.

[24] Hong Kong Privacy Commissioner for Personal Data, Code of Practice on the Identity Card Number and other Personal Identifiers, clause 2.7.

[25] Steve Boggan, "Q. What could a boarding pass tell an identity fraudster about you? A. Way too much", *The Guardian*, 3 May 2006.

2.8 Recommendation 35: Trans-border data flows

Recommendation 35 directly addressed the question of trans-border data flows, a matter on which the Act is largely silent unlike most privacy laws overseas. Recommendation 35(a) proposed a transfer prohibition notice procedure to meet EU requirements. Recommendation 35(b) proposed that attention be paid to the mechanisms necessary to protect information about New Zealanders transferred to places to where no adequate protection is offered.

The first supplementary report updated the recommendations by fleshing out how the transfer prohibition notice provisions might appear. The update also referred to developments in Australia, notably the introduction of National Privacy Principle 9. That provided that private sector organisations could freely transfer personal information to foreign countries if those countries provided protections substantially similar to the National Privacy Principles but otherwise special protections would be required.

There have been several important developments in the area in the last few years. In this short report it is possible to highlight just three:

- the APEC Privacy Framework
- concerns at access by foreign governments
- Australian developments.

APEC Privacy Framework

The APEC Privacy Framework contains nine privacy principles endorsed by APEC Ministers in 2004.

The key principle dealing with trans-border data flows provides:

> **"Accountability**
> A personal information controller should be accountable for complying with measures that give effect to the principles stated above. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these principles."[26]

This accountability principle is APEC's attempt to address the issues of trans-border data flows in a manner relevant to the complexities of 21st century electronic commerce. In particular, APEC recognised that data no longer flows in neat point to point transfers and is commonly distributed amongst a number of players and places and is accessible globally over the internet or private networks.

The accountability principle approach to addressing the challenges of trans-border data flows that is finding favour in some quarters. APEC was partly influenced to take this approach by the accountability principle in Canada's private sector privacy law.[27] The Canadian law provides that:

---

[26] APEC Privacy Framework, clause 26.

[27] Personal Information Protection & Electronic Documents Act 2000 (PIPEDA) , Schedule 1, 4.1.

> "An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party".[28]

Although it does not have a data export prohibition of the type found in the EU Directive, relying instead upon the accountability principle, Canada's privacy law has been officially recognised as providing an adequate standard of data protection to enable the free sharing of personal data from Europe.[29]

The other feature of interest in the context of the APEC Privacy Framework is found in the guidance for international implementation. This provides:

> **"Cooperative development of cross-border privacy rules**
> 46. Member economies will endeavour to support the development and recognition or acceptance of organisations' cross-border privacy rules across the APEC region, recognising that organisations would still be responsible for complying with local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.
> 47. To give effect to such cross-border privacy rules, member economies will endeavour to work with appropriate stakeholders to development frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between them and among the economies.
> 48. Member economies should endeavour to ensure that such cross border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessarily administrative and bureaucratic burdens for businesses and consumers."[30]

The development of cross-border privacy rules remains a work in progress. In 2007 APEC established a pathfinder project to advance work in this area.

Concerns at access by foreign governments

The Privacy Act provides that information privacy principles 6 and 7 apply to information held by an agency outside New Zealand. The Act also provides that principles 5 and principles 8 – 11 apply to information held by an agency outside New Zealand where that information has been transferred out of New Zealand by that agency or another agency. However, the Act provides that it is not a breach of the principles if an agency is required to take an action by or under the law of any place outside New Zealand.[31] Accordingly, while the Act has some extra-territorial operation, it does not require agencies to act in contravention of applicable local laws when operating in another country.

---

[28] PIPEDA, Principle 4.1.3.
[29] European Commissioner Decision 2002/2/EC of 20 December 2001 on the Adequate Protection of Personal Data provided by the Canadian Personal Information Protection and Electronic Documents Act.
[30] APEC Privacy Framework, clauses 46 – 48.
[31] Privacy Act 1993, section 10.

Information about the citizens of one country stored or processed in another country might become accessible to the law enforcement bodies of that other country. Concerns at this possibility have been significantly heightened since September 2001 as a result of the US government enacting broad laws to mandate law enforcement access to information held by private corporations.

These issues have manifested themselves in a variety of ways over the last several years including:

- Canada became concerned that personal information, including medical information, held in the US might be subject to secret demands under the Uniting and Strengthening America by Providing Appropriate Tools to Interact and Obstruct Terrorism Act 2001 (USA PATRIOT Act). In response to such concerns, the Government of British Columbia amended its privacy law to provide that a government agency must ensure that personal information in its custody or under its control is stored only in Canada and accessed in Canada, except in certain circumstances.[32] The Act also provides that the relevant government minister is to be informed when a government agency or contracted service provider receives a foreign demand for disclosure.[33]
- Governments have sought to obtain information about airline passengers for border security and transport safety purposes. Data is used both to profile passengers to identify higher risk passengers for extra scrutiny and to pre-screen and prevent people who are not entitled to enter the destination country from boarding a plane. The issues surrounding the transfer of passenger name record (PNR) data has been, in the absence of clear international agreement, a matter of particular dispute between the EU and US.[34] New Zealand has needed to address these issues in terms of bilateral or regional arrangements for the transfer of New Zealand passenger data.[35]
- The Society for Worldwide Inter-Bank Financial Telecommunications (SWIFT) is a global financial messaging service that facilitates international money transfers. SWIFT stores all messages at operations centres, one of which is in the USA. In mid 2006 it became apparent the at the US Treasury had issued subpoenas requiring SWIFT to provide access to message information held in the USA. This became a matter of significant international controversy and led to investigations by many data protection authorities.[36] As a result of the collective action by data protection authorities of the EU states, SWIFT reformed its arrangements to provide a better level of data protection.[37]

The benefits of modern electronic commerce include the advantages inherent in being able to process data on a 24/7 basis anywhere in the world. However, when information

---

[32] Freedom of Information and Protection of Privacy Act 1996 (FOIPOP), section 30.1.

[33] FOIPOP, section 30.2.

[34] See, for example, Article 29 Working Party, Joint Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes presented by the Commission on 6 November 2007, 5 December 2007 (WP145). This is the latest in a series of reports going back several years.

[35] Customs and Excise Act 1996, section 281; Immigration Act 1987, section 141AA

[36] See Article 29 Data Protection Working Party, Opinion 10/206 on the Processing of Personal Data by the Society for Worldwide Inter-Bank Financial Telecommunications (SWIFT), 22 November 2006.

[37] See Article 29 Data Protection Working Party, press release in relation to the 62nd meeting (9-10 October 2007), 11 October 2007. This records that the clear progress made by SWIFT from a European perspective, especially on technical aspects of compliance with data protection principles.

leaves one's own country and is subject to the laws of another, there is the possibility of governmental access that may not accord with general expectations. There are significant issues at stake which have not yet been adequately resolved at international level.

Australian developments
Australia's privacy law differs from New Zealand in having a trans-border data flow principle applying to private section organisations. The objective is to ensure that information about Australians is protected when transferred offshore.

The main development to note in this context is that the Australian Law Reform Commission has reviewed the trans-border data flow principle. Particularly noteworthy are recommendations that:

- the principle should apply not only to private organisations but also to public sector agencies (with some resultant changes to the principle to recognise governmental interests)
- develop the law consistently with the accountability principle found in the APEC Privacy Framework and Canadian law
- promote transparency by requiring offshore transfer practices to be revealed under a new 'openness principle'.[38]

In exploring mechanisms to give effect to recommendation 35(b), particular regard should be had to the APEC accountability principle.

2.9 Recommendation 36: Proposed Criminal Disclosure Act

Generally speaking, the information privacy principles are not able to be directly enforced in a court of law. Instead, if a question of non-compliance arises, a complaint can be taken to the Privacy Commissioner and afterwards, if appropriate, proceedings can be commenced in the Human Rights Review Tribunal. There is an exception in relation to the right of access under principle 6 which in some cases, can be enforced directly in court. This continues an arrangement established in 1982 which allowed subject access rights under the Official Information Act to be enforced against government departments in the High Court. There was no recommendation in the 1998 report to fundamentally alter this arrangement.

Sometimes when cases are before the courts there are advantages in enabling relevant access rights to be enforced by the court as they control the case. Indeed, this routinely happens in respect of criminal cases before the courts. Although principle 6 may not be explicitly mentioned in these proceedings, defence counsel obtaining documentation from prosecutors on behalf of clients and the enforcement of those arrangements through the court are an example of the enforcement of rights recognised in section 11.[39]

One anomaly identified in *Necessary & Desirable* related to private prosecutions where section 11 could not be relied upon to give the courts statutory power to enforce subject access rights. In this respect it should be noted that the general area of criminal disclosure will be thoroughly reformed by the enactment of a Criminal Disclosure Act.

---

[38] See Australian Law Reform Commission Discussion Paper 72, *Review of Australian Privacy Law*, Chapter 28. Note that the ALRC proposals may change when its final report is submitted.
[39] The courts in effect are enforcing principle 6 rights in tandem with common law rights and Official Information Act entitlements.

The provisions of that proposed Act were contained in the Criminal Procedure Bill introduced in 2004 and which has been reported back with amendments by the Law and Order Committee. The new law will establish a fourfold disclosure regime requiring initial then full disclosure by the prosecution, disclosure of certain information by the defence, and disclosure in certain circumstances by third parties.

The proposed law consolidates a complex body of common law and legislation, including the Privacy Act. When finally enacted, there will be two amendments to the Privacy Act:[40]

- Section 29(1) will be amended to insert a new reason for refusing an access request in circumstances where the request is made by a defendant, or a defendant's agent, and is for information that can be sought under the Criminal Disclosure Act or which has been disclosed to, or withheld from, the defendant under that Act;
- Section 31 – which had never been brought into effect but anticipated limiting access rights to prisoners – will be repealed.

The proposed Criminal Disclosure Act will, once enacted, give effect to recommendation 36.

2.10 Recommendation 37: Independence

Necessary & Desirable discussed the need for institutional mechanisms to guarantee and reinforce the independence of statutory officials. The relationship between the Commissioner, the Ministry and the Minister was noted as were the merits of the alternative Officer of Parliament model. A recommendation was made by the then-Commissioner that there should be provision for the Commissioner to put a case for funding directly to Treasury and relevant Ministers.

Circumstances have changed and it is now my opinion that this recommendation should not be implemented. The law governing these arrangements has since been thoroughly reformed by the Crown Entities Act 2004. That Act makes provision for a class of 'Independent Crown Entities' for which a standard set of legislative and administrative machinery is established to guarantee independence while achieving governmental objectives.

I therefore withdraw recommendation 37.

2.11 Recommendation 37B: Audit developments and powers

Under section 13(b) the Privacy Commissioner has the function of performing audits but only 'when requested to do so by an agency'. No agency has asked to be audited. The audit function has therefore not been performed. *Necessary & Desirable* outlined some of advantages of auditing as a proactive tool for enhancing compliance while recounting some of the challenges. Highest amongst the challenges was the cost. It was frankly acknowledged that since the office had no available resources to devote to developing expertise and systems in this area of work it would have been difficult to undertake audits at that time even if agencies had requested.

The then-Commissioner recognised the merits of audit but did not make a recommendation as he considered that the time was not yet right. In my view things

[40] Criminal Procedure Bill, clause 54.

have now moved on to the extent that it is now appropriate to promote more active consideration of privacy audit. While some progress can be made, and indeed has been made, without changing the law I am of the view that significant progress can only be made with the change in the law and make a new recommendation to that effect.

Although this is not the place to discuss the role of audit in detail, a brief quotation from an internationally respected privacy expert is useful to set the scene:

> "Data Protection Commissioners are a form of highly specialised ombudsmen with a more active part of play than the classic role of responding to individual complaints. It is not enough to respond to repeated similar grievances from a changing cast of individuals. The staff has to pursue general systematic improvements in information handling practices by using a variety of methods."[41]

Private Sector / Public Sector
While the section 13(1)(b) function may now be seen as a fairly timid approach to auditing, it was at the time a reasonably daring innovation.

Amongst privacy commissioners in English speaking countries, there appeared in 1993 to be no ready precedent for commissioners having audit powers in respect of private sector organisations. Indeed, five years later when its Data Protection Act 1998 was enacted, the United Kingdom adopted an 'on request' model just like New Zealand. However, our law was too timid in failing to recognise that Australia and Canada already empowered their privacy commissioners to conduct audits of public sector organisations without the excessively high trigger point of awaiting a request.

Indeed, Australia already had audit powers conferred on the Privacy Commissioner for one small but significant specialist area of the private sector where the Privacy Act applied: credit reporting. Thus for many years the Australian Privacy Commissioner has been able to audit the practices of major credit reporting companies, including those that operate in New Zealand, while the New Zealand Commissioner cannot do so without receiving a request. The Australian Commissioner can also audit, in relation to credit reporting requirements, the practices of credit providers (such as banks) that have access to credit reporting databases.

New Zealand was the first country outside Europe to enact an omnibus privacy law covering both the public and private sectors. It may well have been the right decision at that time to take a cautious approach to audit powers for private sector agencies (although *Necessary & Desirable* notes that a mere three years later Hong Kong was willing to take that step when enacting a law which was modelled on New Zealand's).

I briefly survey some developments of interest in New Zealand, Australia, Canada and the United Kingdom.

New Zealand
There have been developments in the use of privacy audits in two notable areas in New Zealand: information matching and credit reporting.

---

[41] David Flaherty, *Protecting Privacy In Surveillance Societies*, 1989, page 400.

In the information matching area, the Office of the Privacy Commissioner has promoted the use of internal audit. Audit reports are copied to the Privacy Commissioner as part of processes linked to the granting of authorisations or annual review. This approach has been found to be useful for at least two reasons. First, it is cost effective in terms of the Commissioner's resources, as departmental audit staff are undertaking the field work and audits. Second, while maintaining independent oversight, the approach internalises compliance within departmental practices and this encourages 'buy in' to the findings.

The first area where this approach was used was in relation to the granting of on-line transfer approvals. Information Matching Rule 3 prohibits the use of on-line computer connections in an authorised information matching programme unless the Commissioner's approval is obtained. The approach developed in granting approvals has been to attach a condition that an audit report be submitted prior to the expiry of the approval demonstrating compliance with the conditions of the approval. Initial approvals typically run for one year and if a 'clean' audit report is received, a further approval for three years is typically granted (and an audit required before the expiry of that further approval). Thus in 2006/07 some 8 initial approvals and 5 further approvals were granted.[42] Those further 5 approvals each had a satisfactory audit report.

The Office of the Privacy Commissioner has also introduced an audit approach to a limited number of the 46 authorised information matching programmes currently operating. This resulted from a re-evaluation several years ago of the practices then employed by the office for overseeing active matches to identify cost effective ways of continuing a credible level of oversight with a rapid expansion in the number of operating programmes. For certain types of matches, it was also believed that a self-audit approach would provide a better level of oversight than previously employed methods. An audit kit was piloted in 2005/06 and rolled out in 2006/07 to some 16 operating programmes. A revised audit kit for the current year was released in February 2008.[43]

In December 2004 I issued the Credit Reporting Privacy Code 2004. This regulates the commercially important, but privacy sensitive, practices of credit reporting agencies. Agencies involved in credit activities, particularly credit providers, pool sensitive information about customers' identities, credit and defaults, in credit reporters' databases. These large databases contain vast amounts of information and are accessed and updated by many thousands of subscribers. As part of improvements in the regulation of these databases, I determined that audit had a key part to play in promoting better data quality and compliance with privacy controls. The code achieved this by placing an obligation on credit reporters to have internal audit programmes in relation to both data quality requirements and access controls.[44] Agencies wishing to have access to credit reporting databases, must as a condition of the subscriber agreement agree to be audited by the credit reporter in relation to the provisions of the code.

Australia

As earlier mentioned, the Australian Privacy Commissioner has general audit powers in the public sector and specific powers in relation to the credit reporting. The Commissioner has various other audit powers relating to, for instance, the use of the tax

---

[42] Privacy Commissioner, *Annual Report 2006/07*, tables 8 and 9.

[43] The audit kit is available online at www.privacy.org.nz.

[44] Credit Reporting Privacy Code 2004, rules 5, 8, 11 and schedule 3.

file number.[45] As in New Zealand, the Australian Privacy Commissioner may only audit a private sector organisation if the organisation requests it (although the Australian Commissioner does have a power not possessed by the New Zealand Commissioner, to examine the records of private sector organisations).[46] The Australian Law Reform Commission has examined the matter in detail and, without rehearsing the arguments here, has recommended that the Australian Privacy Act be amended to empower the Privacy Commissioner to conduct audits in the private sector.[47]

Canada

Canada enacted privacy legislation to cover the private sector some seven years after New Zealand. The Canadian Privacy Commissioner has power to conduct audits of private sector organisations under the Personal Information Protection and Electric Documents Act (PIPEDA) 1985.[48] This Act provides that the Canadian Commissioner may on reasonable notice and at any reasonable time, audit the personal information management practices of an organisation if the Commissioner has reasonable grounds to believe that the organisation is contravening particular provision of the Act.[49] Having the audit power predicated upon reasonable grounds to believe a contravention possibly takes the Canadian law outside the mainstream thinking on audit as a general compliance tool into the more routine range of enforcement tools. With that particular trigger, the audit approach may not be entirely dissimilar to the existing New Zealand power to commence an investigation on a suspicion of an interference with privacy. However, an audit may have a wider brief than an investigation of particular action or practice.

United Kingdom

As already noted, the UK Information Commissioner's power to conduct audits on private sector organisations has a similar limitation to that on the New Zealand Privacy Commissioner – an audit can only be done with the organisation's consent. The UK Information Commissioner has recently called for stronger powers to allow the Information Commissioner's office to carry out inspections and audits of organisations without the organisation's consent.[50] That worthy recommendation was not immediately adopted. However, late in 2007 Britain was rocked by a security breach involving the loss of 25 million records by a government department.[51] Amongst the responses to this event was a government proposal to expand the Commissioner's audit powers. In an interim report reviewing government data handling procedures, the UK Cabinet Office recorded that the UK government had decided to grant powers to the Information Commissioner to permit 'spot checks' on central government departments and should commit to extending this to the entire public sector. Further consultations are proceeding on how this can be best achieved and funded.[52]

---

[45] For a convenient description of the Australian Privacy Commissioner's audit powers, see Australian Law Reform Commission, *Review of Australian Privacy Law: Discussion Paper 72*, September 2007, page 1211.

[46] *Ibid*, page 1212.

[47] *Ibid,* pages 1216 -1218 and proposal 44-6. Note that the detail of the ALRC recommendation may change before its final report is issued.

[48] The Canadian Privacy Commissioner also has power to conduct audits on government bodies under the Privacy Act 1985.

[49] PIPEDA, chapter 5.

[50] Information Commissioner, *Evidence Submitted to the Home Affairs Committee Inquiry into 'Surveillance Society?'*, 23 April 2007.

[51] Information Commissioner, Press Release, 17 December 2007.

[52] Cabinet Office, *Data Handling Procedures in Government: Interim Progress Report*, December 2007.

In my view, the Commissioner should have mandatory audit powers. Exactly what shape those powers should take warrants further study. It is fair to say that even if the powers are extensive, any Privacy Commissioner will be bound to carefully prioritise audit activity and is likely to conduct only a modest number each year. It is quite likely that audits in the public sector would be one priority. Particular areas such as credit reporting and health information systems would initially be others. There would be no wish to conduct surprise inspections and requirements such as those existing in Canada for audits to be 'on reasonable notice and at any reasonable time' are certainly appropriate limits. One of the reasons for a mandatory requirement is to enable the Office of the Privacy Commissioner to plan an audit programme with some certainty – this simply would not be possible while awaiting agencies to invite the Commissioner in. Having a mandatory power would not preclude promoting other worthy audit initiative such as encourage self-audit, as the Commissioner would never hope to audit more than a fraction of the total number of agencies.

Recommendation 37B
The Privacy Commissioner should have mandatory audit powers in relation to at least the public sector but preferably both public and private sectors.

2.12 Recommendation 46A: Follow through on periodic reviews

Necessary & Desirable was the report of the first periodic review carried out under section 46. As that section was being utilised for the first time, it is unsurprising that no recommendation for change was made. The discussion in the 1998 report pointed out such a review provision was reasonably common in privacy laws around the world. The dynamic environment in which privacy laws operate encouraged law makers to establish a process to return to the subject periodically with the assistance of a systematic expert review. The privacy environment has become even more dynamic, with rapid developments and convergence in technology, communications and science. In my view it is therefore appropriate to continue to have a review provision.

Subsequent experience has revealed some problems that were not anticipated in 1998. In particular, after the Commissioner completed the tasks of undertaking the review as required by statute and submitting the report to the Minister to be tabled in Parliament, the process seems to have stalled. Quite clearly, the framers of the legislation would have expected that the required recommendations be considered and, if accepted, acted upon. The then-commissioner did all that he could to facilitate that process by, for example, submitting a completed typescript to the Ministry of Justice some six months before the published report (then in production stages) was submitted to enable a flying start on the evaluation of the recommendations.

However, nearly 10 years after the report was submitted, and hopefully on the verge of having at least some of the recommendations brought to Parliament in an implementing bill, there is still no public transparency in terms of a position taken by the government on each of the recommendations.

This has, in turn, made it impracticable for a start to be made on a second periodic review required by section 26. If a review were to be prematurely started, the Commissioner and any person engaging in that review would be hampered by not knowing how the previous recommendations were to be treated. Indeed, the Law Commission currently working on its privacy reference will now be facing this very

challenge. The delay in commencing a second review also means that some of the lessons learnt in the subsequent 10 years, or new problems revealed, are not being proactively identified and addressed in the way that the framers of section 26 anticipated.

I make these observations aware of the unavoidable pressures both on departmental officials and on any systemic law reform agenda. However, if Parliament requires periodic reviews of this law to be undertaken then it does seem necessary to have appropriate official follow through. It is unsatisfactory that the recommendations have been put aside for a decade. It is unsatisfactory that there is no transparency in the process after the Commissioner has submitted a report. The various stakeholders should rightly expect to know what has happened to the recommendations identified to make the law work better.

The solution, I suggest, is an approach modelled upon the one recently introduced for governmental responses to reports of the Law Commission. Section 26 should be amended to provide not only that the Privacy Commissioner complete a review and submit a report at certain intervals, and that that report should be promptly presented to Parliament, but also that a governmental response be tabled within a set period – I suggest six months after receiving the report. The periodic reviews could continue to be undertaken at five yearly intervals but 'starting the clock' when the government response is available.

It may be possible to achieve the same outcome without amending section 26 through the Cabinet Office processes or possibly Parliamentary Standing Orders.

> ***Recommendation 46A***
> *Section 26 should be amended so that a government response to the Privacy Commissioner's recommendations is required to be presented to Parliament within six months of receipt and that subsequent reviews should be at five year intervals after a government response is available.*

2.13 Recommendation 50: Trade secret definition

The Privacy Act grants individuals important rights to seek access to personal information about them held by agencies. The Act also sets out a series of good reasons for refusing such requests. One such reason, contained in section 28(1)(a), concerns cases where the release of the information would disclose a trade secret.

It is, of course, difficult to conceive of circumstances where personal information about an individual can be a 'trade secret' that can be withheld from that individual. Thus the earlier recommendation suggested that section 28(1)(a) should be repealed as unnecessary. The recommendation went on to suggest that if the provision were retained, a straightforward definition of 'trade secret' should be inserted. The third supplement noted that the simple definition of 'trade secret' now found in the Crimes Act would be suitable.

On reflection, I no longer support the repeal of the trade secret provision. Although its usefulness may be limited to a tiny number of cases, I now consider that its repeal might cause new problems. There may still be value in providing a simple definition of 'trade secret'. I advised the Ministry of Justice in December 2004 that I no longer wish to pursue the first part of recommendation 50 concerning the repeal of section 28(1)(a).

Accordingly I modify recommendation 50 so that it reads as follows:

> ***Recommendation 50***
> *…[A] straightforward definition of 'trade secret' should be inserted into [section 28].*

2.14 Recommendation 59: Access rights of prisoners

Section 31 of the Privacy Act has never been brought into force. Had it been, it would have restricted the rights of the prisoners from exercising subject access rights. *Necessary & Desirable* noted how problematic that provision appeared to be given the fundamental importance of access rights both to individuals and as an accountability mechanism on government. One need only reflect upon past miscarriages of justice uncovered through prisoners ultimately obtaining access to information from government files.

For some years there has been the desire for comprehensive criminal disclosure regime (sometimes called criminal 'discovery', the term used in civil litigation) and in 2004 a Criminal Procedure Bill was introduced into Parliament. When that law is ultimately enacted, it would have been possible to bring section 31 into effect. Instead, a more sophisticated solution has been developed whereby section 31 will be repealed but a new provision will be included in the Act allowing for access requests to be refused where the criminal disclosure regime should be used (i.e. before or during a trial) or where the criminal disclosure regime has already been used (i.e. the individual has already been given the information or has, under a court supervised process, already properly been refused the information). The new law should be a useful reform in this context.

The Criminal Disclosure Act, once enacted, will give effect to recommendation 59.

2.15 Recommendation 66: Vexatious litigants, etc.

One of the most fundamental rights in any information privacy law is subject access: the entitlement of the individual to find out if an organisation holds information about him or her and seek access to it. The right is central to personal autonomy and to holding organisations accountable. The Privacy Act 1993 introduced access rights for individuals to information held about them in the private sector and continued access rights that previously existed in the public sector under official information legislation.

Necessary & Desirable discussed the possibility of misuse of access rights. That discussion drew upon submissions to the Commissioner and the Commissioner's own knowledge through complaints handling and other interactions with agencies. The discussion in the report outlined how the Privacy Act diminished the potential for misuse. For example, the Act contains provision, not always found in overseas laws, whereby requests can be refused if frivolous or vexatious.

While there is no evidence of widespread misuse of access rights, a small number of individuals have the potential to wreak havoc if they are so minded. A recommendation was offered to empower the Commissioner or the tribunal to exempt an agency from having to deal with a particular individual's access requests for a fixed period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operations of the agency and amount to an abuse of the right of access. The recommendation was modelled upon existing Canadian law.

There have been no particular developments of note in the area of misuse of access rights. However, it is perhaps useful to briefly reflect on two related areas were a vexatious individual can create a nuisance. The first is in relation to lodging numerous complaints to the Privacy Commissioner. The second concerns launching legal proceedings before the Human Rights Review Tribunal.

A few individuals do file multiple complaints with the Privacy Commissioner.[53] This unfortunately is the experience of every statutory complaints body. There is no single strategy for dealing with the problem but I have ensured that my staff have training and support in relation to dealing with querulous complainants. I have fairly extensive discretion to discontinue the investigation of a compliant where I believe, for example, that the subject matter of the complaint is trivial or the complaint is frivolous or vexatious or is not made in good faith.[54] However, if I discontinue on a complaint, the individual may correspondingly launch proceedings in the Human Right Review Tribunal as indeed querulous complainants are apt to do.

The first contextual matter to mention in relation to the HRRT is that the legislation under which the tribunal operates is principally found in the Human Rights Act 1993.[55] Accordingly, in this report I do not make any specific recommendations as they would require a wider consideration than merely amending a section or two in the Privacy Act. The Law Commission may be in a good position to consider some of the broader considerations involved.

There is no filing fee for commencing proceedings in the Human Rights Review Tribunal. The first development to note is that as part of a general review of civil court fees, my predecessor had the opportunity to express some views on the question of tribunal filing fees.[56] The departmental proposal then under consideration was the possibility of introducing a $400 filing fee. The Commissioner took the view that such a fee was too high and would act as a barrier to justice and, as a result, the protection of privacy would be diminished. There were various good reasons for supporting the status quo. Nonetheless, the Commissioner indicated that he was not opposed in principle to there been a small filing fee and felt that one that was aligned with the top of the disputes tribunal range, say $100, would seem appropriate. No change was made to the filing fee arrangements as a result of the departmental review. While not pressing for a filing fee to be introduced, I too would not be opposed in principle to there being a small filing fee. I would not wish it to become a barrier to access to the tribunal but it might make potential litigants pause before taking the significant step of launching proceedings.

The second development is a recent decision declaring, for the first time, a litigant before the tribunal to be a vexatious litigant.[57] The judgment put beyond doubt that the High Court had jurisdiction to do this as the tribunal was found to be an 'inferior court' for the purposes of the relevant legislation. The person declared vexatious in this case had

---

[53] The cases of multiple complaints or multiple legal proceedings before the tribunal are not necessarily access cases but can concern allegations of breach of any principle. I mention them in the context of recommendation 66 for convenience.

[54] Privacy Act 1993, section 71.

[55] See, Privacy Act 1993, section 89.

[56] B.H Slane, Privacy Commissioner, Submission on Review of Civil Court Fees; Stage 2 – Human Rights Review Tribunal, June 2003.

[57] Her Majesty's Attorney General for New Zealand v. Christopher Joseph O'Neill HC AK CIV 2007-404-003303 [20 December 2007].

flooded the tribunal with 70 civil proceedings, at one stage comprising some 57% of the tribunal's case load.

When considering recommendation 66, thought should be given to the general issues and developments associated with multiple complaints and vexatious litigants.

2.16 Recommendation 82A: Covert intimate filming

The third supplement noted that the Law Commission were well advanced on a review of secret filming in intimate circumstances. When consulted by the Law Commission, my office emphasised the ways in which new criminal offences could work in tandem with the civil remedies in the Privacy Act to ensure that certain behaviours were not only deterred and punished but also that victims could effectively obtain compensation for violations of their privacy.

One potential barrier to effective remedies under the Privacy Act for covert filming in intimate circumstances is the 'domestic affairs exemption' which could provide an unfortunate loophole in respect of unlawful behaviours by, for example, members of a victim's household. Recommendation 82 recommended limiting the domestic affairs exemption in section 56 in relation to unlawful covert filming.

In 2004 the Law Commission published its report on unlawful covert filming.[58] The Law Commission found intimate covert filming to be a serious invasion of privacy and affront to human dignity. The privacy invasion is exacerbated when people distribute and possess the images gained. New offences were recommended for making, copying, distributing and possessing covertly filmed intimate images. The Law Commission also recommended amendments to the Privacy Act to ensure that all conduct covered by the new offences can also be dealt with as a breach of privacy complaint. In addition to endorsing the Commissioner's earlier recommendation to amend the domestic affairs exemption in section 56, the Law Commission recommended amending section 85 to give the Human Rights Review Tribunal an explicit power when dealing with cases of intimate covert filming, to make orders for forfeiture of any images or any equipment used in making or distributing such images.[59]

In 2006 amendment was made to Part 9A of the Crimes Act 1961, which sets out crimes against personal privacy, to include a new subpart dealing with intimate visual recordings.[60]

It is important that the recommended counterpart amendments to the Privacy Act be made to ensure that the interests of victims are effectively protected as recommended by the Law Commission.

2.17 Recommendation 83A: Catastrophic natural disasters

On Boxing Day 2004 an undersea earthquake triggered a series of devastating tsunamis along the coast of most land masses bordering the Indian Ocean killing more than 225,000 people in 11 countries and inundating coastal communities with waves of up to 30 metres. It was one of the most deadliest natural disasters in history.

---

[58] Law Commission Study Paper 15, *Intimate Covert Filming*, June 2004.
[59] *Ibid*, R5.
[60] See Crimes Act 1961, sections 126G-216N.

In the aftermath, there was a massive effort in terms of disaster relief and to identify victims and survivors. There was a perception in some quarters that data protection laws in the home countries of visiting tourists may have made the task of trying to identify survivors more difficult. I have no evidence of such a problem arising in New Zealand although there were reports of some difficulties in Australia[61] and Canada.[62] Some of the initial accounts related to incidents on the days when officials and their normal advisers were on vacation.

On 23 August 2005 Hurricane Katrina struck New Orleans which flooded as the levee system catastrophically failed. The hurricane was the costliest in the history of the United States and at least 1,836 people lost their lives. There was criticism of aspects of the disaster management. Issues were raised in the aftermath about the information management of hundreds of thousands victims who were temporarily settled across the United States.[63] Although no amendments to the Federal privacy laws were recommended, a later review did identify various ways in which more proactive approaches to managing the information could be achieved.[64]

Both these events were unprecedented in their scale. It is hardly likely that any information law will perform to its best under such strains.

One result of the Boxing Day tsunami was an amendment to the Australian Privacy Act to insert a new Part 6A to make special provision for the collection, use and disclosure of personal information in emergencies and disasters.[65] In essence, the provisions enable an emergency declaration to be made for the purposes of the Privacy Act. When such an emergency declaration is in effect, certain actions that would otherwise be prohibited may be permitted.

In reviewing the Act in 1998 my predecessor did not explicitly consider issues in relation to major disaster management. It was not an issue that had raised any operational issues at that point.[66]

---

[61] According to an account of evidence given by the Department of Foreign Affairs to a Senate Enquiry, DFAT had the task of tracking down 14,000 Australians who were thought to be in the region after the tsunami struck. It was reported that while there was good cooperation between government agencies, the Privacy Act limited the role of the private sector and that an impediment was probably found in gaining access to airline information. See 'Tsunami prompts call for Privacy Law loosening', ABC News, 20 May 2005.

[62] In Canada it had been reported that foreign affairs officials had invoked Canada's Privacy Act as a blanket reason for not releasing the names of the 146 Canadians missing and feared dead. However, the Canadian Privacy Commissioner made a public statement that this had been a misunderstanding and that the Privacy Act does allow exceptional release of names where there is a public interest that outweighs an invasion of privacy. See 'Naming the missing not a privacy issue', *Victoria Times Columnist*, January 2005.

[63] Particularly challenging, was the coordination of medical treatment and reimbursement of medical expenses as thousands of patients were distributed across the country. The federal medical privacy law (known informally as HIPAA) places an emphasis on patient consent for certain disclosures which may have been impracticable in these circumstance. One particular regulatory initiative taken was for the Secretary of Health to grant a 'section 1135 waiver' which relieved agencies of sanctions and penalties for failure to comply with certain aspects of the federal privacy regulations during the implementation of a hospital's disaster protocol. The Department of Health and Human Services also issued several bulletins giving guidance on compliance with HIPAA in response to Hurricane Katrina.

[64] See The White House, *The Federal Response to Hurricane Katrina; Lessons Learned*, February 2006.

[65] Privacy Act 1998, sections 80F – 80T.

[66] Some issues in relation to the disaster at Cave Creek were the subject of inquiry but it was concluded that the Act caused no difficulties on that occasion and that existing Police policies, which quite properly restricted release of unverified information, worked as they should on the day albeit that short delays in

I am not aware of any significant problem. However, it is important that all reasonable precautions be taken to facilitate disaster relief and the appropriate communication of information about disaster victims and survivors to their relatives. If there is a potential problem, it is desirable that this be identified and an appropriate strategy devised. I am aware that government officials in the last few years have been reviewing disaster preparation in such areas as pandemics. Given that the Australian Privacy Act has so much in common with ours and that the Australian government thought it necessary to amend its law, I raise this as a matter that deserves consideration although I am not sure whether any particular amendment need be made.

Recommendation 83A

Officials responsible for disaster management in New Zealand should give consideration to whether any amendment to the Privacy Act is desirable to provide for best practice disaster information management in the event of a declared emergency and, in particular, whether any amendments such as those adopted in Australia are useful.

2.18 Recommendation 107A: Cross-border cooperation between privacy enforcement authorities

In the third supplement in December 2003, I recommended that the Act be amended to provide for the transfer of complaints to, or the cooperative handling of complaints with, privacy commissioners or similar authorities in other states. I mentioned that this was a development anticipated by the OECD Privacy Guidelines of 1980 and would make sense in terms of building trust in e-commerce.

There have been notable developments in the last four years which strengthen the case for action in this area.

In 2004, the APEC Privacy Framework was endorsed. Part B II of the framework is devoted to cross-border cooperation in investigation and enforcement. Member economies are encouraged to develop cooperative arrangements and procedures to facilitate cross border cooperation in the enforcement of privacy laws. This includes giving attention to mechanisms for effectively sharing information necessary for successful cooperation in cross border privacy investigation and enforcement cases.

In accordance with the spirit of the APEC Privacy Framework, but within limits of existing law, I entered into a Memorandum of Understanding with the Australian Privacy Commissioner in September 2006.[67] That MOU is not solely focused upon cooperation in the area of complaints, but seeks to:

- enhance the exchange of information and cooperation between the offices
- promote cross-border cooperation in investigation and enforcement
- assist each other in training, education, promotion, policy and other activity
- provide a practical means to meet cooperative aspirations set out in the APEC Privacy Framework.[68]

---

release were stressful to some families. See Submission by the Privacy Commissioner to the Commission of Inquiry into the Collapse of a Viewing Platform at Cave Creek near Punakaiki on the West Coast, 5 October 1995.

[67] Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner, 4 September 2006.

[68] MOU, clause 2.1.

Our two offices are currently reviewing the MOU after 18 months experience and this may result in further innovations. However, it is unlikely we can further facilitate the transfer of complaints or information sharing on particular investigations without an amendment to the law as anticipated by the Recommendation 107A.

One country has taken significant steps in this area in recent years. In December 2006 President Bush signed the Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act 2006 (US SAFE WEB Act) into law. The new law grants additional authority to the Federal Trade Commission to help protect consumers from internet fraud and deception through enhancing cooperative enforcement arrangements with foreign privacy and consumer law enforcement authorities. The Act is premised on the fact that the internet and electronic commerce know no boundaries, that cross-border fraud and deception is a growing problem and that US authorities need to cooperate, if regulatory responses are to be successful. The Act has a range of provisions including:

- broadening reciprocal information sharing
- expanding investigative cooperation
- obtaining more information from foreign sources
- protecting the confidentiality of FTC investigations
- protecting certain entities reporting suspected violations of law
- confirming the FTC's remedial authority in cross-border cases
- clarifying FTC authority to make criminal referrals
- providing for foreign staff exchanges
- authorising expenditure of funds on joint projects.

The OECD has taken the initiative at international level through the endorsement in 2007 of an OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. My office contributed to the development of that resource through the OECD Working Party on Information Security and Privacy. As with the US law and the Australian-New Zealand MOU, the focus is not solely on transfer of complaints or requesting enforcement assistance but also covers other areas of cooperation. It focuses upon:

- domestic measures to enable cooperation, particularly by providing effective powers and authority and improving the ability to cooperate
- international cooperation, particularly mutual assistance, engaging in collective initiatives to support mutual assistance and cooperating with other authorities and stakeholders.

The OECD is continuing to work on practical tools to complement the Recommendation and plans to develop a system of national contact points and a on-line platform for enforcement cooperation.

In the particular context of recommendation 107A, the OECD recommendation states:

> 'Member authorities should take steps to improve the ability of their privacy enforcement authorities to cooperate, upon request and subject to appropriate safeguards, with foreign privacy enforcement authorities, including by:

(a) providing their privacy enforcement authorities with mechanism to share relevant information with foreign authorities relating to possible violations of laws protecting privacy
(b) enabling their privacy enforcement authorities to provide assistance to foreign authorities relating to possible violations of their laws protecting privacy, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.'[69]

In implementing recommendation 107A, careful attention should be paid to the recent OECD recommendation on cross-border cooperation.

2.19 Recommendation 108: Complaints backlog

Four years worth of complaints data was available at the time of the Commissioner's 1998 report. Already at that time, it could be seen that the complaints process was under considerable strain with insufficient resources to process complaints in a speedy manner. While hard working the staff at the Office of the Privacy Commissioner were closing many cases - almost 1,000 in 1995/96 and over 800 in 1996/97 - the complaints were arriving in even larger numbers. Statistics published in *Necessary & Desirable* showed, for example, that number of complaints on hand per investigator grew from 50 to 150. The number of complaints carried forward at year end on 30 June 1997 was almost 1,000. Recommendation 108, which called for adequate funding to be made available to process the volume of complaints, was made at a time that the delay in having an investigation *commenced* was 12 months. The position later worsened to a delay of 18 months.

It is therefore pleasing to note that in the last three years things have improved as a result of special backlog funding and baseline budget increases and internal process improvements to 'work smarter'. Thus, for example, at the end of 2002/03 year there were 1,052 complaints carried forward. At the end of the 2006/07 year, only 394 complaints were carried over. The ability to get on top of the complaints backlog has also been helped by the fact that the number of new complaints received currently is substantially lower than was the case up until 2003/04.

Particularly heartening, for complaints staff, complainants and respondents alike, has been the reduction in very old complaints. The total number of files over 12 months has been reduced significantly and 80% of complaints received in 2006/07 were completed, settled or discontinued within 12 months of receipt.

Accordingly, recommendation 108 has been given effect to.

2.20 Recommendations 118 & 119: Information matching

Recommendations 118 and 119 sought to align some of the definitions, and terminology, in Part 10 of the Act with the notion of computer matching. The office now has more experience in these matters and I advised the Ministry of Justice in December 2004 that I no longer supported those recommendations.

---

[69] OECD Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy, June 2007, clause 12.

It is true that most of what is regulated under Part 10 is computer matching. It is also true that many people involved in information matching programmes in New Zealand refer to the practice as 'data matching' – the term that was recommended to be adopted in the law. On reflection, I consider that Part 10 should retain the possibility of regulating manual as well as computerised matches. Some matches, although involving computers, will continue to have a manual element and I would not wish a law change to make the Part 10 framework less useful as a safeguard with those matches.

I therefore withdraw recommendations 118 and 119.

2.21 Recommendations 144: Secrecy provision and the Director of Human Rights Proceedings

Recommendation 104 proposed that section 96 be amended to apply to former Commissioners and employees. Nothing specific had been recommended in respect of the Director of Human Rights Proceedings.

Section 96(1) does not currently apply to the Director since it does not appear that the Director could properly be considered a person "engaged … with the work of the Commissioner". In my view, section 96(1) should be applied to the Director. In particular, I note that Human Rights Act 1993, section 130(1), provides equivalent protection to section 96(1) when the Director is exercising comparable functions under that Act.

The extension of the section 96 privilege to the Director acting in Privacy Act litigation functions is appropriate in its own terms. However, the additional, and key significance is that making that change will automatically apply section 166 to the Director.[70]

Extending the secrecy provision to the Director will place the Director in a similar position to the Privacy Commissioner in resisting demands for information that he holds. In that way, the Privacy Commissioner can share files with the Director confident that the information will not lose its legal protection. The Director will be able to resist a request from the individual concerned under the Privacy Act, or from a third party under the Official Information Act, for access to that information. If the Director initiates proceedings before the tribunal he may, of course, be required to disclose relevant information in accordance with the rules of discovery but the existence of section 116, while not a final determinant, will weigh heavily with the tribunal or any court contemplating ordering discovery. In the absence of an application of section 116 to the Director, the Office of the Privacy Commissioner is under a difficulty in sharing its entire file with the Director in cases that are referred to him. This diminishes efficiency and effectiveness.

Accordingly, I recommend that the position of the Director of Human Rights Proceedings be considered when recommendation 144 itself is considered or implemented. I note, in passing, that the recommendation refers to the possibility of amending schedule 1 of the Privacy Act. With the changes to the Act made by the Crown Entities Act, that schedule is probably no longer the place to make such amendments.

---

[70] See Privacy Act 1993, section 116(1).

Accordingly, recommendation 144 should now read as follows:

> ***Recommendation 144***
> *Section 96… should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner. Provision should also be made for the Director of Human Rights Proceedings.*

2.22 Recommendation 148: Impersonation, etc.

Unlike many overseas privacy laws, there are very few criminal offences in the Privacy Act. Instead, the Act emphasises the duties of agencies to follow responsible information standards and provides individuals with statutory processes to enforce their entitlements and obtain redress when those standards are breached and the individual is harmed as a result.

Notwithstanding the merits of the Privacy Act's civil law approach, there are some areas where criminal sanctions are appropriate. For example, criminal offences to back up the predominately civil approach– the principal example being the offence of hindering the Commissioner in the exercise of powers or refusing the Commissioner's lawful requirements.[71] There are also offence provisions where Parliament deems it necessary to make clear that an unacceptable practice is viewed particularly seriously and is to be deterred and punished. These offence provisions are typically in other statutes and a example is the prohibition on the interception of private communications.[72]

While not wishing to see to a fundamental shift from a civil to criminal approach, *Necessary & Desirable* and supplementary reports did highlight circumstances where new criminal offences would usefully improve New Zealand's privacy law. One such example is where an agency deliberately destroys documents in order to evade an access request.[73]

Recommendation 148 suggested that there be an offence of intentionally misleading an agency by impersonating the individual concerned or misrepresenting the existence or an authorisation from the individual concerned in order to obtain information. Several overseas precedents were mentioned. The case for such an offence provision remains strong and it should be noted that very worrying practices have been exposed in other countries involving the systematic misleading of agencies in order to obtain information.

In May 2006 the UK Information Commissioner released a special report to Parliament entitled *What Price Privacy?*[74]. The report exposed an extensive illegal trade in confidential personal information. The Information Commissioner has proposed ways of improving the situation but has been able to take enforcement action through existing criminal provisions in the UK Act.[75]

Disturbing practices have also been exposed in North America. For example, in the United States during 2007 legislation was introduced at state and federal level to make it an offence to use pre-texting techniques to obtain, sell or solicit others to obtain phone records following various scandals. In Canada, the Privacy Commissioner conducted an

---

[71] Privacy Act 1993, section 127.
[72] Crimes Act 1961, sections 216A-216F.
[73] Recommendation 149.
[74] HC1056.
[75] Data Protection Act 1998 (UK), section 55.

investigation into the practices of LocateCell.com that had circumvented custom authentication procedures of Bell telephone and Telus Mobility. LocateCell.com had used 'social engineering' which is a collection of techniques used to manipulate people into performing actions or divulging confidential information. Pre-texting is one such technique and is the act of creating and using an invented scenario to obtain information from a target, usually over the telephone.[76] The Canadian government has announced plans to amend the criminal code to take concrete steps to address identity theft by, for the first time, creating explicit penalties for collecting, processing and trafficking in personal information.[77]

There continues to be a strong case to criminalise the behaviours identified in recommendation 148.

2.23 Recommendation 152: Coerced access to medical records

The 1998 report highlighted the problem of coerced access and disclosure in relation to medical records. Coerced access involves a third party compelling the individuals concerned to exercise their subject access rights and to pass the information obtained on. Coerced authorised disclosure involves individuals being required to authorise the release of records to a third party. *Necessary & Desirable* mentioned that there had been a growing problem of employers and insurance companies insisting upon individuals exercising access rights to their health records and delivering a copy to the employer or the insurer. It noted that this differed from the reasonable requirement for individuals to undergo a medical examination by the employer's or the insurer's medical practitioner.

It was noted that the problem had also arisen in the UK and that a clause was proposed in their new Data Protection Bill to avoid contractual provisions that purport to require an individual to supply health records obtained under subject access rights. It was recommended that a similar provision be inserted into the Privacy Act. By way of update, the provision mentioned in *Necessary & Desirable* has now been enacted in the Data Protection Act 1998 (UK).[78]

The problem has continued to manifest itself and there have been recent expressions of concerns from patients and professional associations as to the aggressive practices of some insurance companies in seeking access to medical records. I am currently inquiring further into the matter.

I reiterate the desirability of a provision such as proposed in recommendations 152.

---

[76] Privacy Commissioner of Canada, 'Disclosures to Data Brokers Expose Weaknesses in Telecom's Safeguards', PIPEDA Case Summary no.372, 10 July 2007.
[77] Privacy Commissioner of Canada, 'Statement on Government Identity Theft Measures', 22 November 2007.
[78] Data Protection Act 1998, section 57.

3. SUMMARY OF ADDITIONAL AND AMENDED RECOMMENDATIONS

3.1 The following additional recommendations are made:

Recommendation 23A
The Privacy Act should include an obligation requiring agencies to notify affected individuals where a security breach by the agency puts the individual at risk.

Recommendation 25B
Consideration should be given to the merits of a national system, established under statute, to control the use of automated dialling machines and enable individuals to opt-out of telemarketing.

Recommendation 28A
The Law Commission or officials, in further reviewing principle 12, should usefully have regard to:
(a) the Australian experience and proposals with its identifier principle
(b) the usefulness of including exceptions to principle 12(2)
(c) the merit of including controls in principle 12 to encourage number truncation or other ways of controlling the public display of unique identifiers.

Recommendation 37B
The Privacy Commissioner should have mandatory audit powers in relation to at least the public sector but preferably both public and private sectors.

Recommendation 46A
Section 26 should be amended so that a government response to the Privacy Commissioner's recommendations is required to be presented to Parliament within six months of receipt and that subsequent reviews should be at five year intervals after a government response is available.

Recommendation 83A
Officials responsible for disaster management in New Zealand should give consideration to whether any amendment to the Privacy Act is desirable to provide for best practice disaster information management in the event of a declared emergency and, in particular, whether any amendments such as those adopted in Australia are useful.

3.2 In addition, small adjustments are made to recommendations 50 and 144 to read as follows:

Recommendation 50
…[A] straightforward definition of 'trade secret' should be inserted into [section 28].

Recommendation 144
Section 96… should be amended so that the obligation of secrecy clearly extends to former Commissioners and persons formerly engaged or employed in connection with the work of the Commissioner. Provision should also be made for the Director of Human Rights Proceedings.