

Chapter 14

Trans-border data flows

- 14.1 Technological innovation and globalisation have facilitated a surge in trans-border flows of information. The internet, in particular, has enabled information to be moved around the world almost instantly.¹²⁷⁴ These developments have major implications for the protection of informational privacy, and create significant challenges for national information privacy laws like the Privacy Act 1993.
- 14.2 This chapter looks at the international context and the current legal position in New Zealand with regard to the transfer of personal information across borders. It considers options for law reform to better provide for the protection of privacy in relation to trans-border data flows, and then looks at specific issues relating to cross-border cooperation for the enforcement of privacy laws, and steps that might need to be taken to implement the APEC Privacy Framework.

- BACKGROUND**¹²⁷⁵ 14.3 Trans-border data flows are increasingly prevalent in modern commerce and government and individuals may frequently not even realise that their information is being sent overseas. Some examples of trans-border data flows are:¹²⁷⁶
- Businesses and governments are increasingly outsourcing activities, including the processing of personal information about their customers and citizens.
 - Even where a transaction ostensibly takes place within New Zealand, information may often be routed through overseas computer servers. This is often the case with, for example, email and credit card details used to make online purchases.
 - Technologies such as search engines, cloud computing and voice over internet protocol can all involve personal information being sent overseas.

1274 New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) 158.

1275 We have previously discussed some of these issues in New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) chapter 7.

1276 Examples taken from Marie Shroff, Privacy Commissioner “Privacy and Sovereignty: Data fight or flight?” (Address to GOVIS 2007 – Innovation in ICT, Wellington, 10 May 2007) 2–4; Jennifer Stoddart, Privacy Commissioner of Canada “Privacy Protection in a World of Trans-border Data Flows” (Paper presented to Working Party on Information Security and Privacy (OECD), Paris, 3 October 2005); David Loukidelis, Information and Privacy Commissioner for British Columbia “Trans-border Data Flows & Privacy – An Update on Work in Progress” (Address to 7th Annual Privacy & Security Conference, Victoria (BC) 10 February 2006).

- A mirror image of all New Zealanders' passport data is stored in Australia to facilitate the advanced passenger processing system. Immigration New Zealand accesses passports information through Sydney.
 - Motivated by concerns about terrorism and national security, governments are demanding more information about people entering their countries. Airline passenger information about all international air travellers, including ticketing and bookings, is transmitted electronically to Atlanta. The US Department of Homeland Security has sought access to this global database for anti-terrorism purposes.
- 14.4 Paul Swartz has noted some important recent changes in the way international data transfers are occurring. These are:¹²⁷⁷
- A change in scale. Formerly, companies generally worked with discrete, localised data sets, data processing systems were generally nationally-based and an international data flow was an exceptional event. Now, trans-border data flows are continuous and multipoint, and there has been massive growth in the complexity and volume of these flows.
 - A change in processing. Formerly, an international data flow occurred at a predictable moment and into a database controlled by a single entity. In contrast, data transmissions now occur as part of a networked series of processes, and increasingly occur on demand. New technologies allow significant flexibility as to how data flows occur. For example, computing activities can be shifted from one country to another depending on load capacity, time of day and a range of other factors.
 - A change in management. Corporate data processing is becoming professionalised and businesses are now investing more resources in this area.
- 14.5 It will be evident that trans-border data flows can entail significant opportunities for agencies, but that there are corresponding privacy risks. Some countries where personal information about New Zealanders is sent may not have laws in place to protect privacy to the standard that New Zealanders expect. This could result in personal information being exposed. New Zealanders may also not be able to exercise the same rights to seek redress as they can in New Zealand. As the Organisation for Economic Co-operation and Development (OECD) has noted:¹²⁷⁸

When personal information moves across borders it may put at increased risk the ability of individuals to exercise privacy rights to protect themselves from the unlawful use or disclosure of that information. At the same time, privacy enforcement authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities of organisations outside their borders.

1277 Paul M Schwartz "Managing Global Data Privacy: Cross-border Information Flows in a Networked Environment" (Paper to OECD Working Party on Information Security and Privacy, Paris, 12–13 October 2009).

1278 Organisation for Economic Co-operation and Development *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007) 4.

- 14.6 The State Services Commission, in guidance for agencies on off-shoring, has usefully outlined the potential privacy risks that can arise from sending personal information overseas for processing. They include:¹²⁷⁹
- non-compliance with Privacy Act;
 - unauthorised release of personal information;
 - inability to provide data subjects with access to their personal information;
 - inability to cooperate with the Privacy Commissioner over complaints of interference with privacy;
 - inability of the Privacy Commissioner to investigate or enforce against offshore offenders;
 - inability to guarantee the protection of personal information in countries that do not have privacy/data protection laws;
 - foreign laws that conflict with the Privacy Act or offer less protection for the privacy of personal information;
 - a particular country's laws that may enable its government to gain access to New Zealanders' personal information without the knowledge or authorisation of the New Zealand government;
 - overseas judicial decisions that might require disclosure of New Zealand personal information held offshore, or allow the commercial use of that information;
 - problems with recovery and/or secure disposal of personal information at the termination of an outsourcing relationship; and
 - loss of trust in government if government agencies outsource processing of personal information and a data breach occurs
- 14.7 The challenge, then, is to allow trans-border data flows to occur whilst also protecting privacy. A range of international and regional instruments have been developed in pursuit of the twin goals of facilitating free flows of information across borders and protecting privacy. Each seeks to establish consistent rules among countries so that inconsistent national laws do not impede trans-border data flows and economic development.¹²⁸⁰

INTERNATIONAL CONTEXT

- 14.8 A number of international privacy instruments have been developed since the 1980s, with the aim of setting privacy standards to facilitate consistent domestic laws. As yet, however, no international privacy treaty exists, although it is sometimes suggested.¹²⁸¹ The ultimate goal appears to be that all countries will have similar privacy standards, so barriers to trans-border data flows will no longer be necessary. In the interim, international instruments aim to set similar standards for members, so that information flows between member countries can occur unimpeded.

¹²⁷⁹ State Services Commission *Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management* (Wellington, 2009) 6–7, 14–15 and 26–27.

¹²⁸⁰ Blair Stewart, Assistant Privacy Commissioner “The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity?” (Paper to 26th International Conference of Privacy and Data Protection Commissioners, Wroclaw (Poland), 14–16 September 2004) 3.

¹²⁸¹ The International Law Commission has added the topic “Protection of personal data in the trans-border flow of information” on its long term work programme: UNGA “Report of the International Law Commission” (58th Session, 1 May–9 June and 3 July–11 August 2006) A/61/10. Work on this does not appear to be progressing quickly.

- 14.9 The international privacy instruments that are most relevant to New Zealand are those of the OECD, Asia-Pacific Economic Cooperation (APEC), European Union (EU) and United Nations (UN). This section outlines these international instruments as they relate to trans-border data flows, in chronological order. Particular potential reforms arising from them will be discussed in more detail later in the chapter.

OECD Guidelines

- 14.10 The OECD Guidelines,¹²⁸² issued in 1980, form the basis for many countries' privacy legislation, including New Zealand's Privacy Act. The Guidelines aimed to promote trans-border data flows through consistent national legislation. Thus, the recitals recognise:

That although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information ... That automatic processing and trans-border flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices ... That trans-border flows of personal data contribute to economic and social development ... That domestic legislation concerning privacy protection and trans-border flows of personal data may hinder such trans-border flows.

- 14.11 In relation to trans-border data flows, the Guidelines provide that:

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection.

Beyond this, however, they do not prescribe a particular approach that member countries themselves should take in their legislation to deal with trans-border data flows.

¹²⁸² *Recommendation of the Council of the Organisation for Economic Cooperation and Development concerning Guidelines governing the protection of privacy and trans-border flows of personal data* (1980).

Council of Europe

14.12 The Council of Europe's Convention No 108 was adopted in 1981.¹²⁸³ It has been influential, underlying subsequent Council of Europe recommendations and the 1995 EU Directive, discussed below. The Convention may be acceded to by countries outside Europe by a specific procedure.

14.13 Article 12 relates to trans-border flows of personal data, stating:

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation trans-border flows of personal data going to the territory of another Party.
3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
 - (a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
 - (b) when the transfer is made from its territory to the territory of a non-contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

14.14 Protocol 181 to the Convention was adopted in 2001 and deals with cross-border data flows.¹²⁸⁴ Its approach is based on the EU Directive. Article 2 provides that parties may only allow transfers of personal data to non-parties if the receiving state or organisation ensures an adequate level of protection for the intended data transfer.

United Nations guidelines

14.15 The UN produced privacy guidelines in 1990.¹²⁸⁵ They have not been very influential and do not add much to OECD and Council of Europe work. Principle 9 is about trans-border data flows and provides:

When the legislation of two or more countries concerned by a trans-border data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

1283 Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981) CETS 108.

1284 Additional Protocol to the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows (8 November 2001) CETS 181.

1285 UNGA Resolution 44/132 "Guidelines for the regulation of computerised personal data files" (1989) A/44/49.

EU Directive¹²⁸⁶

14.16 The EU Directive¹²⁸⁷ requires EU member countries to prohibit the transfer of personal data to countries that do not have privacy laws meeting the Directive's standards.¹²⁸⁸ Three European Economic Area states (Iceland, Liechtenstein and Norway) that are not EU members are also bound by the directive. Article 25 provides:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place, only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

...

4. Where the Commission finds ... that a country does not ensure an adequate level of protection ... Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

...

6. The Commission may find ... that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into ... for the protection of the private lives and basic freedoms and rights of individuals.

14.17 Data may be exported freely to countries that have been judged to provide an adequate level of protection under article 25(6), without the need for any further controls. This is generally referred to as a finding of "EU adequacy". Countries that currently have this status are Argentina, Canada, Switzerland, the US Safe Harbour scheme and Transfer of Air Passenger Name Record Data, Guernsey, the Isle of Man and Jersey.¹²⁸⁹

14.18 In addition, Article 26 provides for exceptions where transfers may be made even where the third country has not ensured an adequate level of protection. The exception applies where:

- there is unambiguous consent from the data subject;

1286 See also discussion of the Directive in New Zealand Law Commission *Privacy: Concepts and Issues, Review of the Law of Privacy Stage 1* (NZLC SP19, Wellington, 2008) paras 7.43–7.64.

1287 European Parliament and Council Directive 95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.

1288 See generally G Greenleaf "Global Protection of Privacy in Cyberspace – 3. The EU Directive's data export requirements" (Paper to Science & Technology Law Center 1998 Internet Law Symposium, Taipei, 23–24 June 1998).

1289 European Commission Directorate-General for Justice, Freedom and Security "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries" http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (accessed 5 February 2010).

- the transfer is necessary for the performance, implementation or conclusion of certain contractual transaction;
- the transfer is in the public interest or the vital interests of the data subject; or
- the transfer is made from a public register.

Member states may also transfer data where a contract contains adequate privacy safeguards.

- 14.19 So, the fact that a country has not achieved adequacy does not mean that no information may be sent from the EU to that country. However, an adequacy finding simplifies matters considerably. Submitters to the Australian Law Reform Commission's (ALRC) review of the Australian Privacy Act noted that, although not essential for businesses to trade with EU countries, an adequacy finding would help streamline trade between Australian businesses and Europe.¹²⁹⁰
- 14.20 Another aspect of the EU data protection system is the system of binding corporate rules (BCRs), which are similar to APEC cross-border privacy rules, discussed below. BCRs were developed for use by a multinational organisation or group of companies as a mechanism for transferring personal data across borders throughout the organisation under a single standard. BCRs must be approved by every European data protection authority in whose jurisdiction the organisation (or member of the group) will rely on them.¹²⁹¹ Standardised processes and guidance to business have been developed, and data protection authorities are taking a cooperative approach, so that the system is now beginning to work well.

APEC

- 14.21 The APEC Privacy Framework ("the Framework") was endorsed by APEC Ministers in 2004.¹²⁹² It aims to promote electronic commerce by harmonising members' data protection laws and facilitating information flows through the region. APEC members are not obliged to implement the Framework domestically in any particular way.

- 14.22 The Framework establishes a set of ten privacy principles. Principle 9 is the most relevant to trans-border data flows. It provides that a personal information controller:

Should be accountable for complying with measures that give effect to the Principles... 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.

¹²⁹⁰ Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) para 31.31.

¹²⁹¹ See, for example, "The effect of binding corporate rules on overseas transfers of personal data" www.out-law.com (accessed 22 December 2009).

¹²⁹² Asia-Pacific Economic Cooperation "APEC Privacy Framework" (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1.

- 14.23 Another important feature of the Framework is that it allows organisations to develop cross-border privacy rules that apply across the APEC region. The Framework provides:¹²⁹³

Member Economies will endeavour to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

In order to give effect to such rules, member economies are instructed to develop frameworks or mechanisms for mutual recognition of cross-border privacy rules between economies. Such frameworks should “facilitate responsible and accountable cross-border data transfers without creating unnecessary barriers to cross-border information flows.”¹²⁹⁴

- 14.24 The idea of a cross-border privacy rules system has been described as follows:¹²⁹⁵

The aim of an APEC system to protect personal information is to encourage organizations to develop their own internal business rules on privacy procedures governing the movement of personal information across borders. These business rules will apply to an organization's operations and business units throughout the APEC region. Organizations would then be held accountable for complying with their rules by an appropriate authority, such as a regulator. It is these rules developed by organizations that are known as the APEC cross-border privacy rules.

- 14.25 In 2007, the APEC Ministerial Meeting launched the APEC Data Privacy Pathfinder initiative (“the Pathfinder”).¹²⁹⁶ Its purpose is to enable member countries to work together on implementing the Framework, focusing on developing a system of cross-border privacy rules. Member countries cluster into groups in order to “pilot the implementation of cooperative initiatives prior to their adoption by all APEC members.” There are currently nine Pathfinder projects working on developing aspects of the cross-border privacy rules system.¹²⁹⁷ We understand that so far it has proved difficult to translate the idea of cross-border privacy rules into reality. However, the Pathfinder has resulted in the successful completion of the Cross-border Enforcement Cooperation Agreement, which complements the OECD Recommendation discussed below.

1293 Asia-Pacific Economic Cooperation “APEC Privacy Framework” (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1, para 46.

1294 Asia-Pacific Economic Cooperation “APEC Privacy Framework” (16th APEC Ministerial Meeting, Santiago, 17–18 November 2004) 2004/AMM/0114rev1, paras 47 and 48.

1295 Asia-Pacific Economic Cooperation “Project 8 – Scope & Governance of a Cross-Border Privacy Rules System” (Item for 20th Electronic Commerce Steering Group Meeting (DPS), Singapore, 28 July 2009) 2009/SOM2/ECSG/DPS/009.

1296 Asia-Pacific Economic Cooperation “APEC Data Privacy Pathfinder” (Item for Concluding Senior Officials' Meeting, Sydney, 2–3 September 2007) 2007/CSOM/019.

1297 Asia-Pacific Economic Cooperation “APEC Data Privacy Pathfinder Projects Implementation Work Plan” (Item for 17th Electronic Commerce Steering Group Meeting, Lima, 24 February 2008) 2008/SOM1/ECSG/024.

OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy

14.26 The OECD's work on enforcement cooperation has been driven by increasing concerns about the privacy risks associated with the changing character and growing volume of cross-border data flows. Closer cooperation among privacy law enforcement authorities (such as New Zealand's Privacy Commissioner) is seen as a means of better safeguarding personal data. The OECD recommends:

That Member countries co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

- (a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.
- (b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
- (c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
- (d) Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

We discuss the Recommendation, and its implementation in New Zealand, in more detail later in this chapter.

International standards

14.27 A number of organisations are working on developing international privacy standards. The International Organisation for Standardisation has developed an information security standard (ISO 17799) and is also working on developing privacy standards. The International Conference of Data Protection and Privacy Commissioners passed a resolution in 2007 endorsing "the development of effective and universally accepted international privacy standards." The resolution noted that standards have an important role to play, alongside legislation, and that they can be a way of translating "legal requirements into concrete practices."¹²⁹⁸ The Conference continues to promote international standards.¹²⁹⁹

CURRENT SITUATION IN NEW ZEALAND

Privacy Act

14.28 Currently, the main provision in the Act that deals with trans-border data flows is section 10, which provides:

Application of principles to information held overseas

- (1) For the purposes of principle 5 and principles 8 to 11, information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or any other agency.

¹²⁹⁸ Resolution on Development of International Standards (29th International Conference of Data Protection and Privacy Commissioners, Montreal, 25–28 September 2007).

¹²⁹⁹ Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection (31st International Conference of Data Protection and Privacy Commissioners, Madrid, 4–6 November 2009).

(2) For the purposes of principles 6 and 7, information held by an agency includes information held outside New Zealand by that agency.

(3) Nothing in this section shall apply to render an agency in breach of any of the information privacy principles in respect of any action that the agency is required to take by or under the law of any place outside New Zealand.

In addition, agencies must comply with the use and disclosure principles when sending information to anyone, including overseas.

14.29 Furthermore, where an agency holds information solely as an agent, for the sole purpose of safe custody or for the sole purpose of processing the information on behalf of another agency and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency on whose behalf the information is held or processed.¹³⁰⁰

14.30 We note that many New Zealanders share personal information directly with overseas companies over the internet. The law of the country where the company is based will govern the way the personal information in question is treated. Many of the reforms discussed in this chapter, with the possible exception of cross-border enforcement cooperation, will therefore have no application to this type of situation.

EU adequacy

14.31 The EU is currently considering the adequacy of New Zealand's privacy laws. New Zealand has not to date been assessed as adequate, there being two main issues that have prevented it. They are:¹³⁰¹

- The lack of a prohibition on data export, meaning that New Zealand could be a conduit for personal information through which personal information of EU citizens could be sent on from New Zealand to countries without adequate privacy protections.
- Persons outside New Zealand cannot access their own personal information unless they are citizens or permanent residents.

There have also been several smaller points of concern, including the lack of a "sensitive data" concept in the Act and the inability of individuals to opt out of having their personal information used for direct marketing purposes.¹³⁰² However it appears that these are no longer of such concern.

14.32 There have been efforts to secure legislative amendments to address these issues for many years.¹³⁰³ The current Privacy (Cross-border Information) Amendment Bill aims to remove the remaining obstacles to New Zealand achieving adequacy.

¹³⁰⁰ Privacy Act 1993, s 3(4).

¹³⁰¹ See, eg, Blair Stewart "International Transfers of Personal Data: Candidate for Adequacy – The New Zealand Case" (Notes for an address to the Privacy Laws & Business 14th Annual Conference, Cambridge, 3 July 2001).

¹³⁰² The issue of direct marketing is discussed further in chapter 15.

¹³⁰³ See, for example, Office of the Privacy Commissioner *Proposed Amendments to the Privacy Act – addressing question of adequacy under EU Data Protection Directive* (15 December 2000) available at www.privacy.org.nz (accessed 8 October 2009).

Privacy (Cross-border Information) Amendment Bill

14.33 The Privacy (Cross-border Information) Amendment Bill is currently before the House. The Bill amends the Act to ensure that New Zealand is not used as a conduit through which personal information can be sent to states without adequate privacy protection. In doing so, the Bill aims to remove the obstacles to achieving EU adequacy noted above. The key changes it introduces are:

- To allow the Commissioner to prohibit a transfer of personal information from New Zealand to another State if she is satisfied, on reasonable grounds, that:
 - the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Act; and
 - the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines.¹³⁰⁴

This will be achieved by means of a transfer prohibition notice issued by the Commissioner to the agency proposing to transfer the personal information.¹³⁰⁵ Failure to comply with a notice without reasonable excuse will be an offence.¹³⁰⁶

- To allow the Commissioner to consult with an overseas privacy enforcement authority on complaints that are more properly within their jurisdiction, and to refer the complaint, in whole or in part, to that authority.¹³⁰⁷
- To remove the current requirement that a person who makes an information privacy request must be a New Zealand citizen or permanent resident, or be in New Zealand.¹³⁰⁸

14.34 It seems likely that this Bill will pass. This is expected to enable New Zealand to obtain a formal finding of adequacy from the EU.¹³⁰⁹ However, EU adequacy is only one aspect of the issue of trans-border data flows and the Bill's focus is on protections for overseas citizens rather than New Zealanders. The rest of this chapter will consider whether further changes may be needed to deal with trans-border data flows.

EVALUATION OF CURRENT LAW

14.35 As we have seen above, the Act provides some protection where personal information is held overseas. Principle 5 (storage and security) and principles 8 to 11 (accuracy, not keeping personal information longer than necessary, use and disclosure) apply to information held outside New Zealand by an agency. Individuals may, under principles 6 and 7, access and correct personal information held outside New Zealand by an agency.

14.36 If an agency *itself* holds personal information outside New Zealand, principles 5 to 11 apply. If a New Zealand agency sends personal information to overseas agencies that hold information solely as agents, for the sole purpose of safe custody or for the sole purpose of processing information on the New Zealand

1304 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114B).

1305 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114C).

1306 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 8 (new s 114E).

1307 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 7.

1308 Privacy (Cross-border Information) Amendment Bill, no 221-2, cl 5.

1309 Privacy Commissioner "Report by the Privacy Commissioner to the Minister of Justice on the Privacy (Cross-border Information) Amendment Bill" www.privacy.org.nz (accessed 30 September 2009) para 1.4.

agency's behalf, the information is treated as if it was held by the New Zealand agency itself, so the same rules apply. This would seem to cover the case of outsourcing¹³¹⁰ and information sent through overseas computer servers.

- 14.37 If the New Zealand agency gives personal information to an overseas agency, other than one acting as its agent or solely holding or processing information on its behalf, the disclosure to the overseas agency must fall within one of the exceptions to principle 11. If the New Zealand agency does not comply with principle 11, affected individuals could complain to the Privacy Commissioner. However, once the overseas agency has received the information, its holding of it is subject to the laws of the relevant country, which may or may not provide for protection of privacy of the standard expected by New Zealanders.
- 14.38 It seems to us that this is a potential gap in the law. In transferring personal information to an overseas body, agencies are not required to consider whether the personal information will be adequately protected in the overseas destination. This could expose New Zealanders' personal information to an unacceptable level of risk.

Q162 Should there be more protections around personal information being sent out of New Zealand?

HOW SHOULD THE ACT TREAT TRANS-BORDER DATA FLOWS?

- 14.39 There are a number of possible general approaches to the question of how trans-border data flows could be regulated, if at all. We begin by considering the broad approach to dealing with trans-border data flows.

Models for dealing with trans-border data flows

- 14.40 Internationally, a number of approaches exist. These can be roughly grouped into the following categories:¹³¹¹
- no special controls;
 - data export controls;
 - special exceptions; and
 - an accountability model.

No special controls

- 14.41 As the title suggests, under this approach there are no particular special controls on trans-border data flows. This is the approach taken in the USA.¹³¹² At present New Zealand and Hong Kong might also be said to fit into this group, although section 10 of New Zealand's Privacy Act could also be considered

¹³¹⁰ Gehan Gunasekara "The 'final' privacy frontier? Regulating trans-border data flows" (2006) 15 IJLIT 362.

¹³¹¹ These names and groupings were suggested to us by Blair Stewart, Assistant Privacy Commissioner. Another categorisation of models for responding to the challenges of trans-border data flows can be found in Gehan Gunasekara "The 'final' privacy frontier? Regulating trans-border data flows" (2006) 15 IJLIT 362, 378–392.

¹³¹² Although individual organisations may choose to be part of the Safe Harbour Agreement with the EU, whose principles restrict onward transfers of personal information.

to take New Zealand some way towards the accountability model, discussed below. Hong Kong has a section in its law imposing controls similar to the EU, but it has not come into force.

Data export controls

14.42 Under this model, data must not be exported unless it is exported to a country with similar data protection standards to those in the sending country. This is the approach taken in Europe, which we have described above. Argentina¹³¹³ and Australia¹³¹⁴ (in relation to the private sector) have modelled their laws on the EU in this respect.

14.43 In the most restrictive form of this model, data exports could be prohibited entirely. This is the approach taken in relation to the public sector in British Columbia. Public sector agencies must ensure that personal information they hold is stored in Canada and accessed only in Canada, unless the individual consents or it falls within one of the disclosure exceptions.¹³¹⁵ Agency heads must report requests for disclosure that come from overseas to the responsible Minister.¹³¹⁶ This was driven by concerns that information about Canadians could be accessed by US agencies under the USA PATRIOT Act.¹³¹⁷

Special exceptions

14.44 This is the approach taken in the Privacy (Cross-border Information) Amendment Bill. It is based upon clause 17 of the OECD Guidelines, which provides:

A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

Under this model, trans-border data flows are not subject to particular general controls but special exceptions or restrictions can be imposed when the risks warrant it in a particular situation. The Amendment Bill uses the transfer prohibition notice mechanism. Other possible mechanisms could include imposing restrictions on transfers of certain categories of personal information which are particularly sensitive and would not be adequately protected in third countries.

1313 Personal Data Protection Act 2000 No 25.326, art 12.1.

1314 Privacy Act 1988 (Cth), sch 3, cl 9 (National Privacy Principle 9).

1315 Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 30.1.

1316 Freedom of Information and Protection of Privacy Act RSBC 1996 c 165, s 30.2.

1317 See Information & Privacy Commissioner for British Columbia *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Victoria (BC), 2004).

Accountability model

14.45 The accountability model is one that has gained in popularity in recent years. It has been adopted in the APEC accountability principle, discussed above, so can be expected to be influential in the Asia-Pacific region. Under this model, the onus is on an agency to make appropriate arrangements for the protection of personal information if it sends the information overseas. The agency itself will be in breach of the law if it sends information overseas without making such arrangements. New Zealand's section 10 could be seen as following this approach to some extent. It is also the approach taken in Canada, and is likely to be adopted to some extent in Australia and South Africa.¹³¹⁸

Canada

14.46 The Personal Information Protection and Electronic Documents Act provides:¹³¹⁹

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

The Privacy Commissioner can receive complaints about transfers of personal information overseas, and can also audit agencies' practices in this area as part of the Commissioner's general audit function.

14.47 The Privacy Commissioner of Canada has issued guidelines to explain how agencies can fulfil their responsibilities in relation to transfers of personal information to third parties overseas. Agencies must be satisfied that the third party has policies and processes in place, such as staff training and effective security measures, to ensure that the information is protected. The sending agency should also be able to audit or inspect the third party to see how it handles personal information.¹³²⁰

Australia

14.48 The ALRC has proposed a new privacy principle on cross-border data flows that would incorporate the idea of accountability and apply to both public and private sectors. In fact the proposed exceptions mean that the principle is a hybrid of the accountability and data export controls model. The proposed principle states:¹³²¹

If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

1318 South African Law Reform Commission *Project 124: Privacy and Data Protection: Report* (Pretoria, 2009) paras 4.2.26–4.2.37. Also worth noting is the Galway Project, which is devoted to exploring the concept of accountability and how it can fit into broader privacy governance both domestically and internationally: Centre for Information Policy Leadership *Data Protection Accountability: The Essential Elements* (2009).

1319 Personal Information Protection and Electronic Documents Act 2000 c 5, sch 1, cl 4.1.23.

1320 Office of the Privacy Commissioner of Canada *Processing Personal Data Across Borders: Guidelines* (Ottawa, 2009).

1321 Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC R108, Sydney, 2008) recommendations 31-1 and 31-2.

- (a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;
- (b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- (c) agency or organisation is required or authorised by or under law to transfer the personal information.

14.49 The Australian Government has accepted this recommendation, but proposes to modify the exception in (a), adding a requirement that there are accessible mechanisms for individuals to be able to take effective action to have the privacy protections enforced. It also proposes to add the following new exceptions:¹³²²

- (d) the agency or organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to:
 - (i) the individual's life, health or safety; or
 - (ii) public health or public safety
 where in the circumstances it is unreasonable or impracticable to seek the individual's consent;
- (e) the agency or organisation has reason to suspect that unlawful activity or serious misconduct has been, is being or may be engaged in, and the disclosure of the personal information is a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities;
- (f) the agency or organisation reasonably believes that the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law.

14.50 Commentators have criticised the proposed exceptions to the accountability principle, suggesting that they are so wide as to make cross-border data transfers effectively unprotected because most will fall within one of the exceptions.¹³²³ For example, many transfers will take place under a contract, so the principle will not apply (although it might be argued that such contracts will contain adequate safeguards).

Evaluation of models

14.51 All the above models have advantages and disadvantages. The “no special protections” model has the advantages of being simple, requiring no special action and having few compliance costs. However, it is the least effective model in addressing the risks associated with trans-border data flows, leaving New Zealand consumers potentially vulnerable. It also does not meet the expectations of key trading partners, particularly the EU.

¹³²² Australian Government *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (Canberra, 2009) 77–78.

¹³²³ See, for example, Chris Connolly “Weak protection for offshore data – the ALRC recommendations for Cross Border Transfers” (2008) www.galexia.com (accessed 10 February 2009); Karen Dearne “Privacy changes put data at mercy of scams” (20 October 2009) *Australian IT* www.theaustralian.com.au (accessed 24 February 2010).

- 14.52 The “data export controls” model is quite common internationally, so there may be benefits in aligning New Zealand with the model seen as international best practice. It is probably the most privacy-protective model, so would offer relatively strong protection for New Zealand consumers. It has the disadvantages of being relatively costly and complex to operate, and may create barriers to trade and cause political tensions with countries such as the USA. It also emphasises borders as an information control point, which can be artificial.
- 14.53 The “special exceptions” model may take different forms, as outlined above, so potential advantages and disadvantages may vary depending on the form it takes. The model has the benefits of being fairly low cost and likely to be less burdensome for business than other models. It could be seen as targeting the key risk areas. It is also the model already used in the Amendment Bill. Possible disadvantages of this model are that it is uncommon, so may not be trusted by trading partners. It may be seen as providing more limited protection for consumers than more comprehensive data export restrictions. Its exceptional nature means that it may not influence agencies’ practices if it was limited to case-by-case exceptions rather than applying to particular classes of information, for example. The one-off exceptions variant of the model is also dependent upon the regulator learning of risks and taking action, so may not prevent all potential problems. Reforms such as audits that we have suggested elsewhere in this paper may help to uncover problems.
- 14.54 The “accountability” model is consistent with the APEC approach and that of trading partners including Canada and Australia. It has been accepted by the EU in its adequacy finding for Canada. It is a flexible model and gives agencies freedom to find solutions that work for them rather than having external solutions imposed. It also offers a fairly high level of consumer protection. However, it could be viewed as more uncertain than other models.

Options for reform

- 14.55 Based on the above models, we see a number of potential options for reform. They are:
- remain with the status quo (including the Amendment Bill);
 - extend the special exceptions concept so that, for example, transfer prohibition notices could be issued where personal information originates in New Zealand, and/or exports of certain types of information could be restricted;
 - impose data export controls, as in the EU; or
 - adopt the accountability model.

We are interested in hearing submitters’ views on the best approach.

Q163 If you think there should be further reform, which of the approaches discussed in paragraphs 14.40–14.55 do you prefer? Would you prefer another model or variant not discussed here?

14.56 As noted above, one of the difficulties associated with trans-border data flows is that, when information is sent overseas, Privacy Commissioners will not have the same ability to investigate complaints outside their borders, and individuals may not be able to enforce their rights (such as by making a complaint). People may not know how to complain or who to complain to. Cross-border cooperation between enforcement authorities such as Privacy Commissioners can help mitigate these difficulties, for example by:¹³²⁴

- providing information about foreign laws and ways to get redress;
- coordinating access by consumers to the correct privacy complaints body, for example through a shared web portal;
- sharing information about complaints between enforcement bodies in different countries; or
- empowering domestic complaints bodies to transfer complaints overseas.

14.57 We noted earlier in this chapter that many New Zealanders share personal information directly with overseas companies. Cross-border enforcement cooperation may be able to assist in these situations.

OECD Recommendation

14.58 As we have already noted, the OECD has passed a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Its broad recommendations include enabling privacy enforcement authorities to better cooperate with overseas bodies; providing mutual assistance through such methods as notification, complaint referral, investigative assistance and information sharing; developing international mechanisms to facilitate cross-border cooperation; and engaging stakeholders in working towards this goal.

14.59 An Annex to the Recommendation provides more detailed guidance, especially on domestic measures that should be taken to enable cross-border co-operation. These include:

- reviewing and adjusting, where needed, domestic laws to ensure their effectiveness for cross-border cooperation;
- considering ways to improve remedies for those harmed by privacy breaches, wherever they occur;
- considering how domestic privacy enforcement authorities might use evidence, judgments and enforceable orders obtained by an overseas privacy enforcement authority to improve their ability to address the same or related conduct; and
- taking steps to ensure that privacy enforcement authorities have authority to deter, investigate and sanction violations of privacy laws.

¹³²⁴ Blair Stewart “Cross-Border Cooperation on Enforcement Matters” [2004] PLPR 2.

14.60 Of particular note is clause 12, which provides:

Member countries should take steps to improve the ability of their Privacy Enforcement Authorities to co-operate, upon request and subject to appropriate safeguards, with foreign Privacy Enforcement Authorities, including by:

- (a) Providing their Privacy Enforcement Authorities with mechanisms 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.

14.61 The Annex also addresses provision for requesting and giving mutual assistance and collective initiatives to support mutual assistance. This involves naming national contact points, sharing information on enforcement outcomes and participating in enforcement networks. Finally, privacy enforcement authorities are to be encouraged to consult with law enforcement authorities, privacy officers within agencies, civil society and business.

14.62 The New Zealand Act already covers many of these matters. Of particular note is the Commissioner's function of consulting and cooperating with other persons and bodies concerned with the privacy of the individual.¹³²⁵ This seems to provide scope for the Commissioner to cooperate with overseas bodies as well as with domestic bodies, although the exact ambit of the power is not clear. In fact the Commissioner's Office is active in international networks of Privacy Commissioners. Furthermore, new section 72C proposed by the Privacy (Cross-border Information) Amendment Bill will allow the Commissioner to refer complaints to overseas privacy enforcement authorities.

14.63 However, some aspects of the Recommendation may not be adequately covered by existing law (together with the Amendment Bill). It is worth considering whether further amendments are desirable. Particular aspects of the Recommendation that may require further implementation are:

- Enabling OPC to share relevant information with overseas privacy enforcement authorities relating to possible violations of privacy law. This is covered to some extent by the existing law and Amendment Bill. However, the Commissioner does not have clear authority to disclose information to overseas bodies and the Amendment Bill focuses on transferring complaints, which is only one aspect of the proposed information sharing.
- Enabling OPC to provide assistance to overseas authorities relating to possible violations of the overseas country's laws. Some limited cooperation could presumably be provided under the general cooperation function, but again clear authority could be beneficial.
- Provision for requesting and giving mutual assistance.
- Cooperation with other authorities and stakeholders. The Act already provides for the Commissioner to refer complaints to the Ombudsmen, the Health and Disability Commissioner and the Inspector-General of Intelligence and

¹³²⁵ Privacy Act 1993, s 13(1)(j).

Security.¹³²⁶ Furthermore, if during or after any investigation the Commissioner believes that there is evidence of a significant breach of duty or misconduct by any agency or officer, employee or member of an agency, the Commissioner is to refer the matter to the appropriate authority. Again, the question is whether this is sufficient. In future, there may need to be power for the Commissioner to share information with bodies such as APEC accountability agents.

- The Human Rights Review Tribunal may also need powers to consider cases with a cross-border element. If such a case came before the Tribunal, there might be evidential issues not currently provided for. Part 4 of the Evidence Act 2006 establishes a procedure where evidence can be taken in Australia for New Zealand court proceedings and vice versa. The Minister has the power to declare a tribunal a court so that it can also use this procedure. Therefore it would seem that this could be used for trans-Tasman cases. The Evidence Act also makes provision for taking evidence in New Zealand for use in civil proceedings overseas, and vice versa. It may be worth considering whether a similar procedure should be available for the Tribunal.

Q164 Does the Act require further amendments to implement the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy? Are any other amendments required in relation to cross-border enforcement cooperation?

IMPLEMENTATION OF APEC PRIVACY FRAMEWORK

14.64 As described above, the APEC Privacy Framework contains ten privacy principles. Implementation is intended to be flexible, so that member economies are not obliged to take a particular approach. The privacy principles in New Zealand's Privacy Act are similar to the APEC Principles, so New Zealand already complies with much of the APEC Privacy Framework. The possible exception to this is the accountability principle, which we have discussed in paragraph 14.22.

14.65 New Zealand's Individual Action Plan notes provisions of the Act that go some way to fulfil the accountability principle, including sections 10 and 3(4) and principle 11. It then goes on to state that:¹³²⁷

There is no cross-border privacy protection in respect of international transfers of personal information. The Act does not have anything explicit about cross border enforcement cooperation arrangements. Notwithstanding this, the Privacy Commissioner has entered into a Memorandum of Understanding with the Australian Privacy Commissioner which aims to enhance the exchange of information and cooperation between the participants and promote cross border cooperation in investigation and enforcement.

14.66 As discussed above, one option for reform would be to adopt the accountability approach in New Zealand. This would comply with the Framework.

¹³²⁶ Privacy Act 1993, ss 72–72B.

¹³²⁷ Asia-Pacific Economic Cooperation *Information Privacy Individual Action Plan: New Zealand (2008)* www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/dp_iaps.Par.0010.File.tmp/Web_IAP_New_Zealand.doc (accessed 2 November 2009).

Cross-border privacy rules

- 14.67 As discussed above, the Framework envisages the development of a system of cross-border privacy rules (CBPRs), whereby organisations operating across borders would develop their own internal privacy rules to “facilitate responsible and accountable cross-border data transfers” within the organisation. Organisations would still need to comply with local privacy laws.
- 14.68 It is envisaged that the development of cross-border privacy rules will occur in four steps:
- self-certification by companies that their privacy and security practices comply with the APEC Privacy Framework;
 - compliance review of the companies by “accountability agents” that may be APEC-recognised trust marks or government agencies;
 - public notification of compliant companies; and
 - domestic and cross-border complaint handling and enforcement and cross-border privacy laws.
- 14.69 A CBPR system is not yet operational in New Zealand.¹³²⁸ Having such a system could have a number of benefits for New Zealand agencies and consumers. The potential benefits include that it could:
- provide a clearer framework for businesses to operate across borders;
 - be a useful tool to streamline privacy compliance and manage privacy risks for businesses operating across borders
 - be used by businesses participating in the system to gain a marketing advantage;
 - encourage trade, as businesses may be able to trade more confidently with overseas businesses, and overseas businesses may be able to trade more confidently with New Zealand;
 - allow individuals to make an informed choice about the businesses they deal with;
 - assist consumers to enforce privacy rights across borders; and
 - relieve OPC of some work, as businesses/accountability agents took on more responsibility.
- 14.70 However, some potential problems could be:
- it could introduce additional complexity that may increase compliance costs and effort for businesses and be confusing for consumers;
 - the degree to which businesses want such a system, and would be likely to engage with it, is not clear; and
 - there may not be enough privacy experts in New Zealand to perform the various roles required to establish a CBPR system.

¹³²⁸ We are aware, however, of multinational companies with operations in New Zealand that are developing Binding Corporate Rules, the EU equivalent of CBPRs. It is possible that companies that have BCRs could also have these approved as CBPRs under the APEC Framework.

- 14.71 Enabling a CBPR system to operate in New Zealand would require consideration of a number of issues, including:
- Who would be the privacy enforcement authority?
 - Who would be the CBPR accountability agent(s)?
 - What government body would accredit the accountability agent(s)?
 - How would businesses engage with the accountability agent(s)?
 - What form would certification take?
- 14.72 The privacy enforcement authority must be a state body. The obvious candidate is the Privacy Commissioner, although alternatives such as the Commerce Commission could be considered.
- 14.73 The accrediting body for accountability agents must also be a state body. Again, the Privacy Commissioner seems to be a good candidate. Other possibilities might include the Office of the Auditor-General, Audit New Zealand, Standards New Zealand, the Ministry of Economic Development, or a central APEC body.
- 14.74 Accountability agents could be from the public or private sector. The Privacy Commissioner could also perform this role. There could be a role for the private sector, for example, accountancy firms, law firms or existing overseas trust mark bodies such as TRUSTe. Alternatively, a new entity could be set up to be the accountability agent. This could be, for example, a Crown Company or a trans-Tasman body to audit both Australian and New Zealand businesses.
- 14.75 The CBPR system may not necessarily require legislation for its establishment. However, some legislative amendments may be required, for example, to ensure that statutory bodies such as the Privacy Commissioner have sufficient authority to perform their roles in the system, or to establish accountability agents. Additional funding may also be required for the agencies chosen to perform the various roles. The system may be able to be partially funded by participating organisations.

Q165 Do you see value in implementing a cross-border privacy rules system in New Zealand? If so, do you have a view on the questions in paragraph 14.71?

Q166 Do you have any further comments on the issues raised by trans-border data flows?