

# Chapter 7

## Codes of practice

- 7.1 This chapter covers the issuing of codes of practice under Part 6 of the Privacy Act. As discussed in chapter 2, the open-textured, principles-based approach of the Act means that agencies have a great deal of flexibility when it comes to determining how they will comply with the Act. Codes of practice supplement this flexibility by providing a mechanism through which the specific needs and circumstances of particular agencies, businesses, industries, or professions can be accommodated.
- 7.2 In this chapter, we cover:
- the existing framework for issuing codes of practice;
  - an overview of the current codes;
  - a comparison of the Australian and United Kingdom approaches; and
  - some possible changes to the Act.
- 7.3 Under section 63 of the Act, the Privacy Commissioner can issue codes of practice in relation to public registers.<sup>468</sup> Stage 2 of our Review looked at the law relating to public registers.<sup>469</sup> The public register provisions of the Act are therefore outside the scope of this issues paper.
- 7.4 In considering the code-making framework, we do not wish to question the merit or otherwise of any particular code. Specific codes are outside the scope of the review, and we seek comments only in relation to the code-making framework, not the content of any particular code.

---

468 The power has never been exercised. Note, however, that the Credit Reporting Privacy Code 2004, cl 4(2)(b), states that the Code modifies the application of public register privacy principle 2. In addition, authority to issue codes of practice in relation to public registers is conferred on the Privacy Commissioner by sections 122 and 123 of the Domestic Violence Act 1995.

469 New Zealand Law Commission *Public Registers: Review of the Law of Privacy Stage 2* (NZLC R101, Wellington, 2008). The recommendations in this report will be considered by the Government once the Law Commission finishes its review of the Privacy Act. They will be drawn together in our final report.

THE EXISTING  
FRAMEWORK

- 7.5 Part 6 of the Act empowers the Privacy Commissioner to issue codes of practice.<sup>470</sup> A code of practice may apply in relation to information of certain kinds, or in respect of certain kinds of agency, activity, industry, profession, or calling.<sup>471</sup> A code of practice may:<sup>472</sup>
- modify the application of any one or more of the privacy principles by prescribing standards that are more or less stringent than a principle, or exempt any action from a principle unconditionally or subject to conditions;
  - apply any one or more of the privacy principles (but not all of them) without modification;
  - prescribe how any one or more of the privacy principles are to be applied or complied with;
  - impose controls on information matching carried out by agencies that are not public sector agencies;
  - set guidelines to be followed by agencies in determining charges under section 35, and prescribe circumstances in which a charge may not be imposed;
  - prescribe procedures for dealing with complaints of breaches of a code (so long as the code provisions do not limit or revise the provisions in Parts 8 and 9 of the Act); and
  - provide for the review of a code and for its expiry.
- 7.6 By prescribing standards that are more stringent than the standards prescribed by any one or more of the privacy principles, codes of practice can provide enhanced privacy protection. In this way, codes can regulate an area that would otherwise be unregulated. The Credit Reporting Privacy Code 2004, through the limitations that it places on the kinds of personal information that credit reporters can collect, is a good example of this. Conversely, the codes can provide for less stringent requirements than those required by the Privacy Act, thereby effectively exempting agencies or certain sectors from the Act's or the privacy principles' requirements.
- 7.7 The power to issue codes of practice is therefore very wide, but there are limits on what a code of practice could do. For example, a code could not extend the ambit of the Act to agencies to which it does not currently apply, or override or modify other enactments. In addition, a code cannot limit or restrict the rights conferred on individuals by principle 6 and principle 7 to access and correct personal information held by public sector agencies.<sup>473</sup>
- 7.8 Section 53 of the Act sets out the effect of a code. For the purposes of the complaints procedures in Part 8 of the Act, doing something that would ordinarily be a breach of a privacy principle is not a breach if it is done in compliance with a code, and failing to comply with a code is a breach of a privacy principle, even though it would not ordinarily be a breach of such a principle.<sup>474</sup>

---

470 Privacy Act 1993, Part 6.

471 Privacy Act 1993, s 46(3).

472 Privacy Act 1993, s 46.

473 Privacy Act 1993, s 46(5).

474 Privacy Act 1993, ss 53(a) and (b).

- 7.9 The Privacy Commissioner can issue a code of practice on his or her own initiative, or on application by someone else.<sup>475</sup> There are limitations on who can submit a proposed code to the Commissioner for approval and issue.<sup>476</sup> The applicant must be a body whose purpose, or one of whose purposes, is to represent the interests of any class or classes of agency, or of any industry, profession, or calling. The proposed code must be intended to apply either in respect of those whom the applicant represents or in respect of an activity that they undertake.
- 7.10 The Act prescribes the procedure that must be followed before a code can be issued. At a minimum, the Commissioner must give public notice of the intention to issue a code, the details of the proposed code, and information about where copies of a draft of the proposed code can be obtained, and must invite submissions on the proposed code.<sup>477</sup> The Commissioner is required to do everything reasonably possible on his or her part to advise people who will be affected by the proposed code, or their representatives, of the terms of the proposed code, and of the reasons for it.<sup>478</sup> The Commissioner must also give those persons or their representatives a reasonable opportunity to consider the proposed code, and make submissions on it, and must also consider those submissions. These procedures also apply with respect to the amendment or revocation of a code.<sup>479</sup>
- 7.11 The code of practice development process is therefore lengthy and relatively complex. The consultation requirements are a significant part of the process.<sup>480</sup> One commentator has observed that a side benefit of the process is that “agencies requesting the codes are well-versed in their privacy obligations and responsibilities by the time the applicable standard has been reflected within their code”.<sup>481</sup>
- 7.12 A notice must be published in the *Gazette* notifying the issuing of a code of practice, and where copies can be inspected and purchased, and the Commissioner must ensure that copies of a code are available for public inspection free of charge, and for purchase at a reasonable price, while the code remains in force.<sup>482</sup> A code cannot come into force earlier than the 28th day after its notification in the *Gazette*.<sup>483</sup>

---

475 Privacy Act 1993, s 47(1).

476 Privacy Act 1993, s 47(3).

477 Privacy Act 1993, s 48(a).

478 Privacy Act 1993, s 48(b).

479 Privacy Act 1993, s 51(2).

480 The Privacy Commissioner has issued a Guidance Note about codes and the process by which they are made: *Guidance Note on Codes of Practice Under Part VI of the Privacy Act* (Wellington, 1994). The note highlights, in particular, the importance of consultation in the development of codes, not just with industry or professional groups to which the code would apply but also with people about whom information is held.

481 Elizabeth Longworth “Developing Industry Codes of Practice and Policies for the Australian Private Sector” [1996] PLPR 12.

482 Privacy Act 1993, s 49(1).

483 Privacy Act 1993, s 49(2).

- 7.13 Provision is made for the urgent issuing, amendment, or revocation of a code without following the ordinary consultation procedures.<sup>484</sup> Under section 52 of the Act, the Privacy Commissioner can do this if he or she considers that it is necessary to issue, amend, or revoke a code urgently and that for that reason it would be impracticable to follow the ordinary procedure. A code of practice, or an amendment or revocation of a code of practice, issued under section 52 cannot remain in force for longer than one year.<sup>485</sup>
- 7.14 Codes of practice are a form of delegated legislation known as “deemed regulations”.<sup>486</sup> They are issued by the Commissioner rather than by the Parliamentary Counsel Office and do not go through the normal Cabinet approval process that applies to ordinary statutory regulations. The Acts and Regulations Publication Act 1989 does not apply to them, and they are not published in the Statutory Regulations series.<sup>487</sup> However, codes must be presented to the House of Representatives after they are made, and are subject to disallowance under the Regulations (Disallowance) Act 1989.<sup>488</sup>

## CURRENT CODES

- 7.15 There are three main codes of practice currently in force:
- Health Information Privacy Code 1994;
  - Telecommunications Information Privacy Code 2003; and
  - Credit Reporting Privacy Code 2004.

We explain each of these in turn below.

- 7.16 In addition, there are two codes of practice that relate to unique identifiers, and modify the application of principle 12 in particular circumstances to allow unique identifiers assigned by one agency to be used by another. These are as follows:
- Superannuation Schemes Unique Identifier Code 1995; and
  - Justice Sector Unique Identifier Code 1998.
- 7.17 To date, three codes have been revoked or have expired.

### Health Information Privacy Code 1994

- 7.18 The Health Information Privacy Code (HIPC) has the broadest application. It applies to “health information” held by a “health agency”, both terms being very widely defined. A code relating to health information was first issued as a temporary code in July 1993, and was replaced by a permanent code in 1994.<sup>489</sup> The code essentially substitutes a set of 12 rules relating to health information in place of the privacy principles. In some cases, the rules substantially repeat

484 Privacy Act 1993, s 52.

485 Privacy Act 1993, s 52(2).

486 Privacy Act 1993, s 50. For further information on deemed regulations, see “What are Deemed Regulations?” on the Parliamentary Counsel Office website at [www.pco.parliament.govt.nz/what-are-deemed-regulations](http://www.pco.parliament.govt.nz/what-are-deemed-regulations).

487 Privacy Act 1993, s 50.

488 Privacy Act 1993, s 50.

489 The latest edition of the code was published in December 2008, and incorporates Amendment Nos 1-6. Available online at [www.privacy.org.nz/health-information-privacy-code](http://www.privacy.org.nz/health-information-privacy-code).

the provisions of the privacy principles. In others, the privacy principles are modified by adding additional requirements or omitting requirements in a principle that are not relevant in a health context.

- 7.19 The most significant modifications are made in relation to principle 11 (limits on disclosure of personal information), of which rule 11 of the HIPC is the equivalent. Rule 11 supplements the general circumstances set out in principle 11 in which information can be disclosed without the consent of the individual by recognising and codifying what has been described as the “many long-established disclosure practices of the health professions”.<sup>490</sup> An example is information in general terms about the presence, location, condition, and progress of a patient in a hospital, unless disclosure would be contrary to the express request of the patient or his or her representative.
- 7.20 It should also be noted that, although the Act does not usually apply to personal information about deceased persons, section 46(6) of the Act provides that any code of practice relating to health information is to have effect as though principle 11 applied to information about both living and deceased persons. Rule 11 of the HIPC states that it applies to health information about both living and deceased persons, but excludes information about persons who have been dead for 20 years or more.
- 7.21 The complexity of this area of the law is possibly a good justification for having a specific code about health information. The complexity can then, to the extent possible within the limits of a code of practice, be accommodated in a more useful and helpful way than simply relying on the more general privacy principles. The format of a code issued by OPC can also be helpful. The versions of the HIPC issued by the Privacy Commissioner contain a commentary, along with background and explanatory material and practical examples to illustrate the application of the code. These have also been supplemented by other OPC publications such as *On the Record: A Practical Guide to Health Information Privacy*, the second edition of which was issued in July 2000.<sup>491</sup>
- 7.22 A 2002 review by the Mental Health Commission of the way in which District Health Board mental health services are interpreting the Privacy Act and the HIPC found that there is confusion and misunderstanding amongst clinicians about the requirements of the Act and the Code, and their relationship with other key pieces of legislation, such as the Mental Health (Compulsory Assessment and Treatment) Act 1992 and some provisions of the Health Act 1956. Importantly, however, the review concluded that legislative change was not required to address the issues identified.<sup>492</sup> The current legislation was considered to provide a framework which enabled practitioners to make sound decisions on sharing information. What was required was better understanding by staff of the existing legislation pertaining to information-sharing, and clearer

---

490 PDG Skegg and Ron Paterson (eds) *Medical Law in New Zealand* (Thomson Brookers, Wellington, 2006) 299.

491 Office of the Privacy Commissioner *On the Record: A Practical Guide to Health Information Privacy* (2 ed, Wellington, 2000).

492 Mental Health Commission *Review of the Implementation of the Privacy Act 1993 and the Health Information Privacy Code 1994 by District Health Boards' Mental Health Services* (Wellington, February 2002) 10.

information-sharing policies and practices, specific to mental health services. There also needed to be better communication of the current rules and policies, and compliance with both by mental health services staff.

- 7.23 Of the three main codes of practice, the HIPC generates the highest number of complaints. In the 2008–09 year, the Office of the Privacy Commissioner (OPC) received 147 complaints relating to the three principal codes, of which 139 related to the HIPC.<sup>493</sup> This no doubt reflects the broader scope of the HIPC compared with the other two codes of practice. Of the 81 privacy cases that were brought before the Human Rights Review Tribunal between 1993 and 2006, 12 cases (15 per cent) were brought under the HIPC.<sup>494</sup> The highest award of damages to date for a Privacy Act complaint, \$40,000, was made in a case involving the disclosure of health information.<sup>495</sup>
- 7.24 While it appears that the HIPC is generally operating well, experience with the HIPC also illustrates the limitations of a code of practice in an area of law as complex as health information. The code must also coexist and interrelate with a complex web of other health-related legislation, such as sections 22B to 22H of the Health Act 1956, and the Code of Health and Disability Services Consumers' Rights issued under the Health and Disability Commissioner Act 1994, as well as health practitioners' ethical duties and long-standing industry practices.<sup>496</sup> While we include no final view in this paper, we ask in chapter 19 whether health information may need its own, separate legal regime.

### Telecommunications Information Privacy Code 2003

- 7.25 The Telecommunications Information Privacy Code (TIPC) was issued in 2003. The code has its origins in a draft code jointly prepared by a working group of the then principal network operators (Telecom, BellSouth, and Clear Communications). Those operators presented their draft code to the Privacy Commissioner in 1997, and asked the Privacy Commissioner to consider issuing their draft code under the Act.<sup>497</sup> Resourcing issues, coupled with the need for subsequent work by the Privacy Commissioner, prevented the then Privacy Commissioner from advancing the proposed code for some years, and a draft code was not released for public consultation until December 2001.
- 7.26 The TIPC applies to “telecommunications agencies” (which includes network operators, publishers of directories of subscribers of telecommunications services, internet service providers, and mobile telephone retailers) with respect to personal information about subscribers, information generated as a result of a

493 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25.

494 Gehan Gunasekara and Erin Dillon “Data Protection Litigation in New Zealand: Processes and Outcomes” (2008) 39 VUWLR 457, 472.

495 *Hamilton v The Deanery 2000 Ltd* [2003] NZHRRT 28.

496 Some of the complexities of the relationship between the HIPC and section 22F of the Health Act 1956 are explored in Nicola S Peart “Access to, and Disclosure of, Health Information: Are the Rules in Need of a ‘New Treatment’?” (1996) 2 HRLP 95. The Public Health Bill 2007, no 177-2, if enacted, would repeal and replace the Health Act 1956. The provision of the Bill that is equivalent to section 22F is clause 24. We discuss the interrelationship of the Privacy Act and the Health and Disability Commissioner Act in chapter 11.

497 See further Office of the Privacy Commissioner “Telecommunications Privacy Issues in New Zealand 1995–1998” [1998] PLPR 29.

telecommunication, and the content of a telecommunication. To the extent that it applies, the code effectively substitutes 12 telecommunications information privacy rules for the privacy principles, although some of the principles are applied without modification.

- 7.27 The TIPC deals with the inclusion and availability of the contact details of subscribers in or through directories and directory services, and the use of Calling Line Identification Presentation (commonly known as “caller ID”). Restrictions on the use of telecommunications for the purpose of direct marketing are also imposed. Specific provision is made for collection, use and disclosure “for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity.”
- 7.28 The TIPC is reasonably complex, and relies on a number of definitions from other pieces of legislation, particularly the Telecommunications Act 2001. The code is also noteworthy in that it requires telecommunications agencies to set up and operate their own internal complaints-handling process, although this does not displace the right of persons to complain directly to the Privacy Commissioner.
- 7.29 The Regulations Review Committee (RRC) considered the TIPC in 2003/04 and raised concerns about two aspects of the code (as originally issued).<sup>498</sup> The Privacy Commissioner subsequently amended the TIPC to meet these concerns. The RRC was satisfied with the amendments.
- 7.30 Only one complaint relating to the TIPC was received by the Privacy Commissioner in the 2008/09 financial year.<sup>499</sup>

#### Credit Reporting Privacy Code 2004

- 7.31 Credit reporting companies hold vast amounts of information about people. Some of the information held by credit reporting companies is highly sensitive, and reflects on a person’s financial reputation.<sup>500</sup> These companies collect masses of information every day. For example, Veda Advantage, which operates in both Australia and New Zealand, states that it collects data on more than 16.5 million individuals and 4.4 million companies in New Zealand and Australia, and each day generates credit reports on 60,000 individuals and businesses on both sides of the Tasman that apply for credit.<sup>501</sup>
- 7.32 The Credit Reporting Privacy Code (CRPC) was issued in 2004, and became fully operational in April 2006. It has been amended three times, once by a temporary amendment. As with the TIPC, resourcing issues in the OPC in the

498 Regulations Review Committee *Activities of the Regulations Review Committee in 2004* (April 2005).

499 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25. Ten complaints were received in the previous year under the TIPC.

500 Further, most of the information about a person is collected from sources other than the person himself or herself. It has been provided by banks, utility companies such as telecommunications, electricity, and gas suppliers, and retailers, or it is sourced from publicly-available information, for example bankruptcy notices. The information is made available by credit reporting companies to a wide range of agencies, in most cases without the subject of the information knowing about it.

501 Veda Advantage “What We Do” [www.vedaadvantage.com/about-veda/nz\\_about-what-we-do.dot](http://www.vedaadvantage.com/about-veda/nz_about-what-we-do.dot) (accessed 10 February 2010).

late 1990s stalled progress on the code, and a proposed code was not issued for public consultation until 2003. The Privacy Commissioner has noted that the credit industry was fully engaged during the statutory consultation process and in subsequent discussions, making many helpful suggestions about the workability of proposed solutions and ways to minimise compliance costs. As a result, substantial changes were made to accommodate these suggestions.<sup>502</sup>

- 7.33 The CRPC addresses key concerns about credit reporting by:<sup>503</sup>
- limiting the information that may be contained in credit reporting systems
  - controlling who may have access to the information
  - reducing opportunities for misuse
  - enhancing the transparency and openness of the process
  - ensuring that individuals are made aware of their rights and that disclosures are properly authorised
  - establishing standards to avoid mismatching information about different individuals
  - ensuring information is regularly updated
  - requiring access logs to be maintained
  - removing the financial barriers to “self-auditing” by requiring credit reporters to provide individuals on request with free copies of any credit information held about them
  - providing greater certainty about how long information will be retained
  - requiring disputed information to be flagged or suppressed while its accuracy is determined
  - requiring prompt low-level dispute resolution.
- 7.34 A key aspect of the CRPC is the limitation it imposes on information that credit agencies can include in their systems. A credit reporter can only collect personal information for the purpose of credit reporting if the information falls within the definition of “credit information”. The definition includes identifying information about the individual, information about an application for credit (such as the type of credit and the amount sought), credit default information (such as the date of default, the amount in default, and when the amount in default was finally settled), information about any summary instalment orders or judgments for monies owed against the individual, bankruptcy information (adjudications, discharges, suspensions, and annulments), and information sourced from certain public

502 Office of the Privacy Commissioner *General Information Paper on the Credit Reporting Privacy Code* (Wellington, December 2004).

503 Office of the Privacy Commissioner *Privacy Commissioner Annual Report for the year ended 30 June 2006* (Wellington, 2006) 26.

registers. The essential feature of this information is that it is negative in character.<sup>504</sup> It does not include information tending to establish a person's good credit history, such as timely repayment of loans without defaults.

- 7.35 A further feature of the CRPC is that it applies directly only to credit reporting agencies. Credit providers (such as banks and finance companies) and other agencies (subscribers) that obtain credit reports (such as debt collectors, prospective employers, prospective insurers, and prospective landlords) are covered indirectly, through the agreements with credit reporting agencies under which they access credit information. The privacy principles still apply to credit providers and other subscribers.
- 7.36 Compatibility with the way in which credit reporting is regulated in Australia is also a significant issue, given the close relationship between the New Zealand and Australian markets. The Australian Law Reform Commission (ALRC) has reviewed the credit reporting provisions in the Privacy Act 1988 (Cth) and made recommendations for changes to those provisions.<sup>505</sup>
- 7.37 The CRPC provides that the Privacy Commissioner must review the code as soon as practicable after 1 April 2008. A review of the CRPC is currently underway. As part of the review process, the Privacy Commissioner set up a reference group, consisting of a selection of key stakeholders (credit reporting agencies, credit providers, government agencies, privacy experts, and consumer groups).<sup>506</sup> One of the most contentious issues for consideration in the review of the CRPC is undoubtedly whether or not New Zealand should move from its current negative reporting regime to positive or more comprehensive credit reporting.
- 7.38 Seven complaints relating to the CRPC were received by the Privacy Commissioner in the 2008/09 financial year.<sup>507</sup>

---

504 “Negative” and “positive” are terms commonly used in relation to credit reporting. The Australian Law Reform Commission explains them as follows: “As the term suggests, negative credit reporting involves ‘negative’ information – that is, information that detracts from an individual’s credit worthiness, such as the fact that he or she has defaulted on a loan. On the other hand, positive credit reporting is said to involve ‘positive’ information about an individual’s credit position and includes information relating to that person’s current credit commitments. An example of information in this category is a record of an individual having made a loan repayment.” However, the ALRC goes on to caution that this distinction is something of an oversimplification and can be somewhat misleading. Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) 1800–1802.

505 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) chs 52–59. There are currently significant differences between Australian and New Zealand law with respect to whether a credit reporting agency in one jurisdiction can supply a credit report in response to a request made in the other jurisdiction. New Zealand law permits cross-jurisdictional requests for credit reports, but Australian law does not. The ALRC report recommends that the Australian restriction be relaxed in certain circumstances (see recommendation 54–7).

506 See Victoria Hinson, Lazar Associates Ltd *Review of Credit Reporting Privacy Code 2004: Report of Reference Group Discussions – June 2009* (Office of the Privacy Commissioner, Wellington, 2009). The New Zealand Law Commission was a member of the reference group as an independent observer.

507 Office of the Privacy Commissioner *Privacy Commissioner Annual Report 2009* (Wellington, 2009) 25.

A COMPARISON  
OF OVERSEAS  
APPROACHES

7.39 In the following section we examine the approaches to privacy protection through codes of practice in Australia and the United Kingdom.<sup>508</sup>

## Australia

*Federal*

7.40 The original Privacy Act 1988 (Cth) applied only to Federal government agencies, and made no provision for the issuing of codes of practice. The Act was extended to credit reporting agencies and credit providers in 1990, and the Privacy Commissioner was required to issue a code of conduct relating to credit reporting. The Australian Privacy Commissioner issued the Credit Reporting Code of Conduct in September 1991. Compliance with the Code of Conduct is mandatory for credit reporters and credit providers, and breaches constitute an interference with privacy for the purposes of the investigation and enforcement provisions of the Act.

7.41 The Privacy Act 1988 (Cth) was extended by the Privacy Amendment (Private Sector) Act 2000 to cover private sector organisations (which are referred to in the Act as “organisations”, in contrast to public sector “agencies”). As part of that extension, organisations were provided with the option of developing their own privacy codes for the handling of personal information,<sup>509</sup> which, if approved by the Australian Federal Privacy Commissioner, take the place of the National Privacy Principles for the organisations subject to the code. Unlike in New Zealand, the Australian Privacy Commissioner cannot initiate a privacy code, and a code is not binding on organisations that do not consent to be bound by it. Codes will only be approved by the Privacy Commissioner if they provide at least as much privacy protection as the National Privacy Principles; thus, codes cannot provide for less stringent requirements than the Act requires. The approach was “designed to allow for flexibility in an organisation’s approach to privacy, but at the same time, guarantees consumers that their personal information is subject to minimum standards that are enforceable in law.”<sup>510</sup> The inclusion of the privacy code mechanism as part of the extension of the Act to the private sector reflected the government’s view that co-regulation of the private sector with respect to privacy was preferred over self-regulation or full regulation.<sup>511</sup>

7.42 Commenting on the code provisions in the Australian Act, Nigel Waters observed:<sup>512</sup>

It remains to be seen whether private sector organisations find it worthwhile to develop and submit codes for approval. Given that the standards cannot be less than the NPPs, the only advantage to an organization or industry sector in submitting their own principles would seem to be the opportunity to couch them in industry specific

508 Canadian privacy legislation does not make provision for the development of codes and thus is not considered here.

509 Privacy Act 1988 (Cth), Part IIIAA.

510 Office of the Privacy Commissioner (Cth) *Guidelines on Privacy Code Development* (Sydney, 2001) 16.

511 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.2.

512 Nigel Waters “Codewatch: Privacy Codes – What are They? Where are They?” [2001] PLPR 6.

language. In relation to complaint handling, some sectors may perceive an advantage in providing for privacy complaints to be handled in the first instance by an industry specific body (a code adjudicator under the Act), although this advantage was arguably eroded by a late amendment to make determinations of code adjudicators subject to appeal to the Commissioner — replacing a more limited but more powerful right to judicial review.

7.43 At the date of writing, there were only three approved codes listed on the website of the Office of the Australian Privacy Commissioner.<sup>513</sup>

7.44 In a review in 2005 of the operation of the private sector provisions of the Privacy Act, the Office of the Australian Privacy Commissioner made the following comments on the operation of codes under the Act:<sup>514</sup>

Another area where the objectives of the private sector provisions have not been achieved in the way that was anticipated is the adoption of industry and organisation codes by the private sector to regulate their collection, use and disclosure of personal information. There are only three approved codes under the Privacy Act. However, there is no call for the repeal of the code provisions of the Act despite the very low level of take-up. Most businesses appear content to be regulated by the NPPs and to have the Office as their external complaints handling body.

7.45 Submissions to the Office of the Australian Privacy Commissioner as part of that review suggested that the development and approval process for codes was unduly long, onerous, complex, and costly. The Office accordingly recommended that it review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them.<sup>515</sup> The Office also recommended that the Privacy Commissioner be empowered to issue binding codes.<sup>516</sup>

7.46 As part of its review of the Privacy Act, the ALRC sought submissions on the question of codes.<sup>517</sup> The ALRC's report indicates that responses identified support for the existing co-regulation model in the Privacy Act, but also raised issues about the complexity of the privacy regime as a result of voluntary codes, and the resource-intensive nature of the code-making process, which was considered to have little identifiable benefit.<sup>518</sup>

---

513 These are the Market and Social Research Privacy Code, the Queensland Club Industry Privacy Code, and the Biometrics Institute Privacy Code. The website also indicates that one application for approval of a code is currently being considered by the Privacy Commissioner: the Internet Industry Privacy Code. See [www.privacy.gov.au/business/codes/register](http://www.privacy.gov.au/business/codes/register) (accessed 11 February 2010).

514 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005).

515 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005) recommendation 47.

516 Office of the Privacy Commissioner (Cth) *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Sydney, 2005) 46–47.

517 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) ch 48.

518 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.10.

- 7.47 In its recommendations, the ALRC considered that privacy codes under the Privacy Act 1988 (Cth) should operate more like the way in which codes operate in New Zealand. Taking a set of recommended Unified Privacy Principles (UPPs) as the base standard, the ALRC recommended that privacy codes should operate in addition to the UPPs, rather than replacing the UPPs as is currently the case.<sup>519</sup> The Government response accepted this recommendation in principle, but noted that while a code cannot derogate from the UPPs, there was no reason why it should not expand upon or enhance them.<sup>520</sup> To that extent it might “replace” them.
- 7.48 The ALRC did not recommend that the Privacy Commissioner should have power to issue binding codes, despite strong support among stakeholders.<sup>521</sup> The Government response, however, supports a power for the Commissioner to *request* an organisation to develop a code; and then, if an adequate code is not developed, a power in the Commissioner himself or herself to develop and impose a mandatory code.<sup>522</sup> Breach of such a mandatory code would be an interference with privacy under the Act, and subject to enforcement mechanisms.<sup>523</sup>

### *New South Wales*

- 7.49 Under the New South Wales Privacy and Personal Information Protection Act 1998, codes of practice may be initiated and developed by the NSW Privacy Commissioner or any public sector agency, and then submitted to the responsible Minister (currently the Attorney-General).<sup>524</sup> The responsible Minister can then decide whether or not to make the code.<sup>525</sup> Codes are drafted by the Parliamentary Counsel’s Office, made by order of the responsible Minister, and published in the Gazette.<sup>526</sup> Codes can modify the application of one or more of the information protection principles as they apply to any particular public sector agency (the Act does not apply to the private sector) by:
- specifying requirements that are different from the requirements set out in the principles, or exempting any activity or conduct of or by the agency from compliance with any such principle;
  - specifying the manner in which any one or more of the information protection principles are to be applied to, or are to be followed by, the agency; or
  - exempting the agency, or any class of public sector agency, from the requirement to comply with any information protection principle.

519 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) recommendation 48 -1.

520 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 89.

521 Australian Law Reform Commission *For Your Information: Australian Privacy Laws and Practice* (ALRC R108, Sydney, 2008) para 48.34.

522 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 89–90.

523 Australian Government *Enhancing National Privacy Protection. Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (Canberra, October 2009) 90.

524 Privacy and Personal Information Protection Act 1998 (NSW), Part 3.

525 Privacy and Personal Information Protection Act 1998 (NSW), s 31(4).

526 Privacy and Personal Information Protection Act 1998 (NSW), s 31(5).

- 7.50 Importantly, the Act states that codes may not impose requirements on public sector agencies that are more stringent (or of a higher standard) than those of the information protection principles.<sup>527</sup> Agencies to which any particular code applies must comply with its provisions.<sup>528</sup>

## United Kingdom

- 7.51 The Data Protection Act 1998 is the United Kingdom's primary data protection law. An Information Commissioner oversees compliance with the Act. Codes of practice are recognised by the Act as follows:

- Section 51 of the Act imposes a duty on the Information Commissioner "to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers". If directed by the Secretary of State or if the Information Commissioner considers it appropriate to do so, the Commissioner is to prepare and disseminate appropriate codes of practice for guidance as to good practice. Appropriate consultation with trade associations, data subjects or persons representing data subjects must precede the issuing of a code of practice.
- Section 51(4) provides that the Commissioner must, where he or she considers it appropriate to do so, encourage trade associations to prepare and disseminate codes of practice to their members. The Commissioner must also consider any code of practice submitted to him or her by a trade association, and after such consultation with data subjects or persons representing data subjects as appears to the Commissioner to be appropriate, notify the trade association whether in the Commissioner's opinion the code promotes the following of good practice. The term "trade association" is defined as any body representing data controllers.

- 7.52 The Information Commissioner has issued a number of codes of practice under section 51(3).<sup>529</sup> An example of an industry-developed code of practice endorsed by the Information Commissioner under section 51(4) of the Act is the code of practice for archivists and records managers.

- 7.53 Codes of practice issued under section 51 do not have the same legal status as codes of practice issued under the New Zealand Privacy Act. A departure from a code is not unlawful, and the basic legal requirement remains compliance with the Data Protection Act itself. A code sets out the Information Commissioner's recommendations about how to meet the legal requirements of the Act, but data controllers may have alternative ways of meeting those requirements. Enforcement action against a data controller would still be based on a failure to meet the requirements of the Act, but the Commissioner is likely to refer to the Code and ask the data controller to justify any departure from the code.

---

527 Privacy and Personal Information Protection Act 1998 (NSW), s 29.

528 Privacy and Personal Information Protection Act 1998 (NSW), s 32.

529 Code of Practice on Telecommunications Directory Information Covering the Fair Processing of Personal Data (1998); Employment Practices Code (2005); CCTV Code of Practice (2008); Privacy Notices Code of Practice (2009). The Information Commissioner has also issued a Framework Code of Practice on for Sharing Personal Information (2007), which is designed to assist organisations to produce their own code of practice on information sharing.

## Observations

7.54 By comparison with codes of practice in other jurisdictions we have examined, the New Zealand codes of practice are significantly more potent. Codes of practice in New Zealand can modify the privacy principles, can prescribe standards that are more stringent or less stringent, or can exempt actions from the privacy principles. Australian Federal codes cannot prescribe standards that are less than the National Privacy Principles. In New South Wales, codes cannot be more stringent, or impose higher standards on public agencies than the relevant privacy principles require. Codes of practice in New Zealand have legal status, something they do not have under the United Kingdom Data Protection Act 1998. In Australia, at the Federal level, codes are only binding by consent, although that may be about to change.

## OPTIONS FOR REFORM

### General views

- 7.55 Few codes of practice have been issued under the Privacy Act 1993 during the 17 years since the Act was passed. The Privacy Commissioner noted in *Necessary and Desirable* that when the Bill was being enacted it was expected that codes would be required for the banking and insurance industries, but none had been forthcoming.<sup>530</sup> This remains the case.
- 7.56 On this basis, our overall conclusion is that the principles-based approach in the Privacy Act, together with the guidance and advice provided by the OPC, is working satisfactorily for most agencies to which the Act applies, without the need for a code of practice.
- 7.57 This is not to diminish the importance of the code of practice mechanism in the Privacy Act. The codes that have been issued in New Zealand, while small in number, cover some key areas such as the health and telecommunications sectors. The value of a code-making provision as a “reserve power”, to be used if other measures fail, should also not be underestimated. The practice of the current Privacy Commissioner is to try “light-handed” regulatory measures, such as guidelines, first, before escalating to a code of practice.
- 7.58 Subject to what we say below, our research has not uncovered significant problems with the code of practice mechanism in the Privacy Act. It appears to be working satisfactorily, a view shared by the OPC. The limitations, however, on what a code of practice can achieve in an area where privacy is only one part of a complex web of law and practice is apparent from the Health Information Privacy Code.
- 7.59 We consider that most aspects of the code-making process are necessary and desirable, and would not propose to change them. The Privacy Commissioner is an independent statutory officer, and the Commissioner and his or her staff are experts in the field of privacy. It makes sense to bring to bear that independence and expertise in the development of codes of practice. The process of making

530 *Necessary and Desirable* para 6.2.4. The fact that no code has been made under the Privacy Act for the banking and insurance industries could be due in part to the oversight of these industries by the Banking Ombudsman and the Insurance and Savings Ombudsman, established in 1992 and 1995 respectively.

codes of practice is a very public one. The intention to issue a code must be publicly advertised, and submissions on draft codes must be called for and considered. Codes must be publicly notified and made publicly available.

7.60 Nor do we think that the scope of codes of practice should be more restricted. The power to modify the effect of the privacy principles “up or down” provides a desirable degree of flexibility in the Act. While comparable overseas jurisdictions have more limited code-making powers, we do not regard the New Zealand provision as excessive.

7.61 In its submission to the Privacy Commissioner’s 1998 review, the New Zealand Law Society observed:<sup>531</sup>

A huge amount of work, time and resources goes into developing a code of practice. The effect of this expense is seen in the small number of codes that have been drafted. Industries perceive minimal benefits to their consumers, the costs of drafting a code appear to outweigh the benefits. The result is an inaccessible and ineffective code mechanism.

7.62 In the light of our assessment above, we do not think that this was a fair assessment of the code mechanism then, nor is it now. We note that the Privacy Commissioner did not recommend significant changes to the code of practice procedure in *Necessary and Desirable*.<sup>532</sup> In response to suggestions that codes of practice could be developed more quickly and efficiently, and that codes could be simpler and shorter, the Commissioner emphasised the status of codes of practice as pieces of delegated legislation, which alter the legal obligations imposed under statute.<sup>533</sup> They must therefore be issued with the precision expected of legislation and remain within the powers conferred by the Act on the Commissioner. We agree that the “code-lite” approach is not appropriate, and indeed propose below that the status of codes justifies their being made in the same way as ordinary statutory regulations.

7.63 We note that the work involved on the part of the OPC in developing and consulting on a code is very extensive for a small organisation. The early development of some of the codes now in place was hindered by a lack of resources. There is a suggestion that this may still be a problem, and that it is a factor in agency decisions not to invoke the code mechanism. For example, the Ministry of Education identified a code of practice as an alternative to the enactment of Part 30 of the Education Act authorising the use of the National Student Number (NSN). The Regulatory Impact Statement for the Education Amendment Bill 2004 (enacted as the Education Amendment Act 2006) makes the following observation about the code of practice option:<sup>534</sup>

Authorisation Option A – Code of practice under Privacy Act 1993

A code of practice under the Privacy Act 1993 would provide the authorisation of the extension for the NSN, specify permitted purposes and agencies permitted to use the

---

531 Quoted in *Necessary and Desirable* 207.

532 *Necessary and Desirable* Part VI.

533 See for example *Necessary and Desirable* para 6.2.6.

534 Ministry of Education “Regulatory Impact Statement Relating to the National Student Index”, available at [www.minedu.govt.nz](http://www.minedu.govt.nz) (accessed 11 February 2010).

NSN. A code would be subject to the complaints and damages provision in the Privacy Act 1993. A code is not the preferred option as it cannot establish penalties for misuse alone, nor require the compulsory use of the NSN by agencies. A code does not provide the same opportunity for parliamentary debate and decision-making that is desirable for such a widely applied identifier for a compulsory activity, and the centralised collection of personal information associated with the NSN. The development of the code would be managed by the OPC, including consultation. The work programme is determined by the OPC, which is experiencing resource constraints, and this creates some uncertainty for other projects requiring confirmation about the availability of the NSN.

- 7.64 The OPC is now better resourced than when it was first established, but our own involvement on the reference group participating in the review of the CRPC gives us some appreciation of the large amount of work involved in developing and maintaining a code.
- 7.65 Despite our general conclusion about codes of practice, we remain keen to find out whether or not any changes to the Act are required to make the development of codes more effective, or to improve the effectiveness of codes generally. We have not identified any ourselves. We welcome views.

### Codes of practice enacted as ordinary regulations

- 7.66 As we noted above, we are happy with the majority of the code-making provisions and the processes they provide for, but we do consider that added constitutional safeguards should be added to the code-making process.
- 7.67 The code-making provisions in the Privacy Act confer considerable power on the Privacy Commissioner. In constitutional law terms, section 46 of the Act is a “Henry VIII” clause as it confers delegated authority to amend an Act of Parliament.<sup>535</sup> This sort of power should be granted by Parliament “rarely and with strict controls”.<sup>536</sup>
- 7.68 Others have identified this issue as well. We note the submission from the Commonwealth Press Union to the Privacy Commissioner in the context of the *Necessary and Desirable* review.<sup>537</sup>

The provision of codes where specific needs arise is one of the more useful pieces of flexibility available to affected industries or activities under the Act. We note, however, the wide powers of the Privacy Commissioner in drafting, accepting and amending codes of practice. There are significant constitutional issues in giving unelected officials such as the Privacy Commissioner the right to put in place codes which are potentially more restrictive than the law itself.

535 For more on Henry VIII clauses see Legislation Advisory Committee *Guidelines on Process and Content of Legislation* (Wellington, 2001, most recently amended 2007) 205–206.

536 Regulations Review Committee *Report on the Inquiry into the Resource Management (Transitional) Regulations 1994 and the principles that should apply to the use of empowering provisions allowing regulations to override primary legislation during a transitional period* [1995] AJHR I16C.

537 Quoted in *Necessary and Desirable* 203.

- 7.69 Moreover, as well as being Henry VIII provisions, codes do not follow the conventional process for regulation-making in New Zealand. As we noted previously, codes of practice are “deemed regulations”. Ordinary regulations are drafted by the Parliamentary Counsel Office, approved by the Cabinet, made by the Governor-General in Executive Council, notified in the *Gazette*, and published in the Statutory Regulations Series (SR Series) and on the New Zealand Legislation website. Codes of practice, while they are deemed regulations, do not follow this process. Once issued by the Privacy Commissioner, codes have to be presented to the House of Representatives, can be examined by the Regulations Review Committee, and are subject to disallowance (and amendment) under the Regulations (Disallowance) Act 1989. As noted above, the Regulations Review Committee has examined one code of practice and identified issues with it.<sup>538</sup> It was of the view that changes were required, and these were subsequently made to the Committee’s satisfaction.
- 7.70 Having accepted that the breadth of the power to make codes of practice is appropriate, we consider that accountability for the exercise of that power should be brought more into line with established constitutional arrangements. Ordinary regulations are made by the Executive, which has the confidence of the House and is answerable to it. As the Law Commission suggested in its submission to the Regulations Review Committee’s examination of deemed regulations, “the further the law-making power is removed from Parliament and the greater its effect, the more ‘constitutionally obnoxious’ it becomes.”<sup>539</sup>
- 7.71 In making this suggestion, we do not mean to imply that the Privacy Commissioner has in any way abused the powers conferred by the Act. Indeed, the Privacy Commissioner clearly recognises the significance of the powers, and goes out of her way to ensure that the process of code development is open and transparent, and that the final product of a high standard and readily accessible.
- 7.72 We note that the RRC recommended that all deemed regulations be approved by the Cabinet as part of the promulgation process, and that the Government Response to the RRC’s report rejected this recommendation.<sup>540</sup> One of the primary concerns of the RRC in making this recommendation was related to quality assurance. The rejection of that recommendation in the Government Response was based on the inappropriateness of Cabinet processes simply as a quality assurance check. Our recommendation is based on more fundamental constitutional considerations.

---

538 See discussion of the Telecommunications Information Privacy Code above.

539 Law Commission “Submission to the Regulations Review Committee Review of Deemed Regulations”. Noted as submission 30 to the Regulations Review Committee “Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation” (Wellington, 1999) fn 30.

540 See *Government Response to the Report of the Regulations Review Committee on its Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation* (October 1999); see also *Further Government Response to the Report of the Regulations Review Committee on its Inquiry into Instruments Deemed to be Regulations – An Examination of Delegated Legislation* (November 2000).

*Model process*

- 7.73 The sort of model we have in mind is the one incorporated in the Health and Disability Commissioner Act 1994. Under that Act, the Health and Disability Commissioner (HDC) is required to develop a Code of Health and Disability Services Consumers' Rights (CHDSCR).<sup>541</sup> Notification and consultation obligations similar to those contained in the Privacy Act apply to the development of a Code by the HDC.<sup>542</sup> But while the Commissioner proposes, Cabinet disposes. Once a draft Code has been developed, the HDC forwards it to the Minister, who must present it to the House.<sup>543</sup> However, the Code does not become operative unless it is prescribed by regulations made under section 74 of the Act. The same process applies to amendments to the Code.
- 7.74 Indeed, it is possible under the Health and Disability Commissioner Act for the Executive to make regulations prescribing a CHDSCR that differs from the draft developed by the HDC, or contrary to or without the HDC's recommendations. But in that case the Minister must, within 12 sitting days of the making of the regulations, present a statement to the House explaining how the Code differs from that recommended by the HDC, and the reasons for the differences, or (where applicable) the reasons why the regulations were made contrary to or without a recommendation of the Commissioner.<sup>544</sup>
- 7.75 While this model is generally worthy of presentation here it is not entirely appropriate for codes of practice under the Privacy Act. A CHDSCR needs to be in place for the Health and Disability Commissioner Act to work. So the option of prescribing a code that has not been recommended by the HDC has to be available to the Executive. Codes of practice are not essential to the operation of the Privacy Act.
- 7.76 Given the fact that privacy codes of practice can override the Privacy Act, and the importance of consultation in their development, we do not think that the Executive should be able to prescribe a code of practice in relation to a particular area unless the Privacy Commissioner has developed a code for that area and made a recommendation to the Government. The Government should be able to reject the proposed code, but not modify it.<sup>545</sup> If the Government were to reject the code, the Minister should have to give reasons to the House.
- 7.77 We do not see that the proposed new process should significantly affect the existing processes of code development and consultation. In effect, it gets the best of both worlds. It preserves the independence of the Privacy Commissioner, but imposes a greater degree of accountability for the exercise of the legislative function under the Act. There are some potential risks. We have considered whether the proposed new process might jeopardise meaningful participation by industry players in the code development process, and therefore adversely affect the quality of the outcome. The fact that the ultimate power to decide

---

541 Health and Disability Commissioner Act 1994, s 19.

542 Health and Disability Commissioner Act 1994, s 23.

543 Health and Disability Commissioner Act 1994, s 19.

544 Health and Disability Commissioner Act 1994, s 75.

545 The House of Representatives could still amend or replace the code, once incorporated in regulations, through the power conferred by section 9 of the Regulations (Disallowance) Act 1989.

whether a code is implemented or not would lie with the Executive, with the attendant risk that the effort that goes into the development of a code might be wasted if a code is rejected, might discourage engagement. We think that the robustness of the code development process, and the status of the Privacy Commissioner, make this unlikely, but we seek comments on the issue.

- 7.78 A further risk is that, despite the huge effort that goes into the development of a code, internal government processes might derail a proposed code if officials inappropriately seek to relitigate or second-guess the Privacy Commissioner's recommendations. Again, we think this unlikely, given that the Executive would only be able to reject a proposed code, and would have to give reasons publicly for the rejection.
- 7.79 The process we recommend would also mean that codes of practice would be published in the SR Series and on the New Zealand Legislation website. We think that the potentially broad application of codes of practice makes that entirely appropriate. This of course would not prevent the Privacy Commissioner from publishing annotated versions codes with explanatory and guidance material included, as the Commissioner does now.

### Time limits on codes

- 7.80 There is one other change to the code-making procedure that we suggest should be considered. It also arises out of a constitutional issue. As indicated above, codes of practice are made under what amounts to a Henry VIII clause. The Regulations Review Committee (albeit in a different context) has recommended that regulations made under Henry VIII clauses should expire after a certain period (that is, there should be a sunset clause).<sup>546</sup> Section 46 of the Act provides that a code may provide for its review by the Commissioner, and may also provide for the expiry of the Code. Neither a review nor expiry are mandatory. We invite comment on whether or not they should be.

### Significant policy issues

- 7.81 The ambit of the Privacy Act is very wide, covering personal information practices in most areas of the public and private sectors. Codes of practice can have a correspondingly wide application. The flexibility that codes of practice provide to address difficulties in the application of the Act or new issues that arise is, in our view, essential. However, this does not mean that a code of practice will always be the most appropriate way of dealing with an issue. There are some issues that, even though they could be dealt with by a code of practice, might be too contentious or significant to be legislated for in a code. Choosing the right instrument to deal with the issue is important. Although the code of practice process involves significant public input and consultation, sometimes legislation will be more appropriate.

---

<sup>546</sup> Report of the Regulations Review Committee *Inquiry into the Resource Management (Transitional) Regulations 1994 and the Principles that Should Apply to the Use of Empowering Provisions Allowing Regulations to Override Primary Legislation During a Transitional Period* [1995] AJHR I16C.

- 7.82 The National Student Number issue mentioned above is a possible example.<sup>547</sup> In that case, the Ministry of Education noted that, although a code of practice could be used to authorise the extension of the NSN, “a code does not provide the same opportunity for parliamentary debate and decision-making that is desirable for such a widely applied identifier for a compulsory activity, and the centralised collection of personal information associated with the NSN”. In the context of the TIPC, the Regulations Review Committee objected to the inclusion of certain provisions in the original code on the basis that that the enforcement of foreign laws should not be facilitated through a privacy code.
- 7.83 It is clearly impossible to identify in advance what issues might, or might not, be suitable to be dealt with in a code. However, our suggested change to the way in which codes of practice are implemented would assist in addressing this issue. The last word on implementing a code of practice would rest with the Government of the day, rather than the Privacy Commissioner. Cabinet could decide that, even though the Privacy Commissioner has developed a code of practice, a code is not the appropriate mechanism for dealing with the issue, and decline to prescribe the code.

## CONCLUSION

- 7.84 Our overall conclusion is that the code of practice mechanism in the Privacy Act appears to be working satisfactorily. Nevertheless, we welcome comment and feedback on these issues.

Q94 Are any changes to the Act required to make the development of codes of practice more effective, or to improve the effectiveness of codes generally?

Q95 We consider that codes of practice should be implemented by ordinary regulations approved by Cabinet, rather than simply being issued by the Privacy Commissioner. Do you agree?

Q96 Should reviews, or sunset provisions, be mandatory in relation to codes of practice?

<sup>547</sup> See paragraph 7.63 above.